(7)

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-100632
(43)Date of publication of application : 13.04.2001

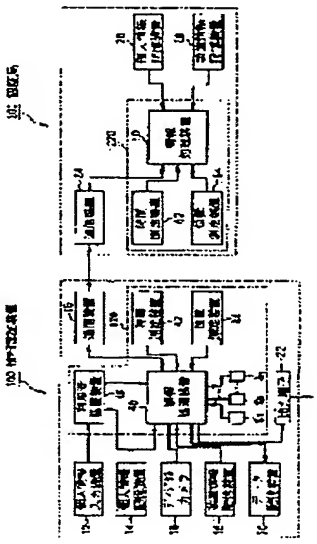
(51)Int.Cl. G09C 1/00
G09C 5/00
H04L 9/32

(21)Application number : 11-280825
(22)Date of filing : 30.09.1999

(71)Applicant : SEIKO EPSON CORP
(72)Inventor : KOBAYASHI MICHIO

(54) INFORMATION AUTHENTICATION DEVICE AND AUTHENTICATION OFFICE

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an authentication device and an authentication office suitable for improving a verification ability as an evidence of data by ensuring objectivity of the data.
SOLUTION: The information authentication device 100 is comprises of a digital camera 10, and an authentication information adding part 120 for adding authentication information to digital data. On the other hand, the authentication office 200 is provided with communication equipment 24 for receiving the digital data from the information authentication device 100 and a digital signature adding part 220, and when the digital signature adding part 220 authenticates that the digital data are inputted with the digital camera 10, based on the authentication information added to the digital data received by the communication equipment 24, it adds a digital signature to the digital data received with the communication device 24.



LEGAL STATUS

[Date of request for examination] 18.03.2004
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

P,2001-100632,A [CLAIMS]

NOTICES *

PO and NCIPI are not responsible for any
lamages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] The information authentication equipment characterized by to have an authentication information addition means add to the data which generated the authentication information for attesting having inputted data as a data input means is equipment which attests data and input data, with said data input means based on the information acquired from the exterior, and inputted this with said data input means.
[Claim 2] It is information authentication equipment which said authentication information addition means has a location measurement means measure a location using an external-information dispatch means, generates the positional information for pinpointing the point which inputted data with said data input means based on the location which measured with said location measurement means in claim 1, and is characterized by to add the positional information which generated as authentication information.
[Claim 3] The information authentication equipment which characterizes by to have an authentication information addition means add the authentication information for attesting having inputted data with a data input means is equipment which attests data using the certificate authority which performs a digital signature, and input data, and said data input means to the data which inputted with said data input means, and the transmitting means transmit the data which added authentication information with said authentication information addition means to said certificate authority.
[Claim 4] It is information authentication equipment which said authentication information addition means has a timing measurement means to measure time amount, generates the hour entry for specifying the time of inputting data with said data input means based on the time amount measured with said timing measurement means in claim 3, and is characterized by adding the generated hour entry as authentication information.
[Claim 5] It is information authentication equipment which said authentication information addition means has a location measurement means measure a location, generates the positional information for pinpointing the point which inputted data with said data input means based on the location measured with said location measurement means in either of claims 3 and 4, and is characterized by to add the positional information which generated as authentication information.
[Claim 6] It is information authentication equipment which said authentication information addition means has an environment condition measurement means measure a surrounding environment condition, generates the environment condition information for specifying the environment condition at the time of inputting data with said data input means based on the environment condition measured with said environment condition measurement means in claim 3 thru/or either of 5, and is characterized by to add the environment condition information which generated as authentication information.
[Claim 7] In claim 3 thru/or either of 6, it has an individual humanity news storage means for memorizing individual humanity news, and an individual humanity news input means to input individual humanity news. Said authentication information addition means It is information authentication equipment characterized by adding the individual humanity news of said individual humanity news storage means as authentication information while the individual humanity news inputted with said individual humanity news input means and the individual humanity news of said individual humanity news storage means are filling predetermined relation.
[Claim 8] It is information authentication equipment which equips the information authentication equipment concerned with the equipment information storage means for memorizing the equipment information which is the information on a proper in claim 3 thru/or either of 7, and is characterized by said authentication information addition means adding the equipment information on said equipment information storage means as authentication information.
[Claim 9] It is information authentication equipment which said authentication information addition means generates the inspection information for inspecting whether the error is contained in the data concerned using the data inputted with said data input means in claim 3 thru/or either of 8, and is characterized by adding the generated inspection information as authentication information.
[Claim 10] It is information authentication equipment characterized by generating inspection information by the Hash Function using the data which inputted said authentication information addition means with said data input means in claim 9.
[Claim 11] It is information authentication equipment characterized by enciphering the data with which said authentication information addition means added authentication information in claim 3 thru/or either of 10.
[Claim 12] It is information authentication equipment characterized by for said cipher system being a public-key-encryption-ized method and said authentication information addition means enciphering the data which added authentication information with the private key of the information authentication equipment concerned in claim 11.
[Claim 13] Information authentication equipment characterized by having a receiving means to receive the data with which the digital signature was added by said certificate authority from the certificate authority concerned, and a data storage means to memorize the data which received with said receiving means, in claim 3 thru/or either of 12.
[Claim 14] A certificate authority side receiving means to be the certificate authority which performs a digital signature to the data transmitted from information authentication equipment according to claim 3 to 13, and to receive data from said information authentication equipment, It has a digital signature addition means to add a digital signature to the data received with said certificate authority side receiving means. Said digital signature addition means It is the certificate authority characterized by adding a digital signature to the data received with said certificate authority side receiving means when it attests having inputted data with said data input means based on the authentication information added to the data received with said certificate authority side receiving means.
[Claim 15] It is the certificate authority characterized by to add a digital signature to the data which received with said certificate authori

le receiving means while the time amount specified by the hour entry added as authentication information on the data which have a
rtificate authority side timing-measurement means to by which said digital signature addition means measures time amount in claim 14,
id received with said certificate authority side receiving means, and the time amount which measured with said certificate authority side
ming-measurement means are filling predetermined relation.
Claim 16] In either of claims 14 and 15 said digital signature addition means While the location pinpointed by the positional information
dded as authentication information on the data which have a certificate authority side location measurement means to measure the
ocation of said information authentication equipment, and were received with said certificate authority side receiving means, and the
ocation measured with said certificate authority side location measurement means are filling predetermined relation The certificate
authority characterized by adding a digital signature to the data received with said certificate authority side receiving means.
[Claim 17] Said information authentication equipment is equipped with the certificate authority side equipment information storage means
for memorizing the equipment information which is the information on a proper in claim 14 thru/or either of 16. Said digital signature
addition means While the equipment information added as authentication information on the data received with said certificate authority
side receiving means and the equipment information on said certificate authority side equipment information storage means are filling
predetermined relation The certificate authority characterized by adding a digital signature to the data received with said certificate
authority side receiving means.
[Claim 18] In claim 14 thru/or either of 17 said digital signature addition means The same method as information authentication equipment
according to claim 9 generates inspection information using the data received with said certificate authority side receiving means. It is the
certificate authority characterized by adding a digital signature to the data received with said certificate authority side receiving means
while the generated inspection information and the inspection information added as authentication information on the data received with
said certificate authority side receiving means are filling predetermined relation.
[Claim 19] It is the certificate authority characterized by generating inspection information by the same Hash Function as information
authentication equipment according to claim 10 using the data which received said digital signature addition means with said certificate
authority side receiving means in claim 18.
[Claim 20] It is the certificate authority characterized by decrypting the data received with said certificate authority side receiving means
with the decryption method with which said digital signature addition means corresponds with the cipher system of information
authentication equipment according to claim 11 in claim 14 thru/or either of 19.
[Claim 21] It is the certificate authority which said decryption method is a public key decryption method, and is characterized by said
digital signature addition means decrypting the data received with said certificate authority side receiving means with the public key of the
information authentication equipment which is the transmitting origin of the data concerned in claim 20.
[Claim 22] The certificate authority characterized by having a certificate authority side transmitting means to transmit the data which
added the digital signature with said digital signature addition means to said information authentication equipment in claim 14 thru/or either
of 21.
[Claim 23] The certificate authority characterized by having a certificate authority side data storage means to memorize the data which
added the digital signature with said digital signature addition means in claim 14 thru/or either of 21.

[Translation done.]

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the information authentication equipment and the certificate authority which attest data, and relates to suitable information authentication equipment and a suitable certificate authority to improve the certification force as a proof of data by securing the objectivity of data especially.
[0002]
[Description of the Prior Art] In recent years, in the United States, the digital image photoed with the digital camera besides the photograph taken with the usual camera is also increasingly accepted as a proof of a trial. However, generally, since the alteration was comparatively easy, digital data, such as a digital image, had the problem that the certification force of proof was inadequate.
[0003] Conventionally, the car control event data authentication equipment indicated by JP,11-115831,A is one of things relevant to the technique which improves the certification force as a proof of digital data.
[0004] This is what records control events, such as a series of operation performed by the operator before the occurrence of a motor vehicle accident, during generating, or after generating. The microcontroller which is combined that control event information should be received, adds the 1st time stamp and a vehicle identification number VIN to control event information, gives the 1st information, and outputs the 1st information to memory by the time overlap method, The memory which is combined with a microcontroller and a microprocessor and stores the 1st information and the 2nd information by the time overlap method, When it is combined with memory and two or more transducers, it judges whether the received collision data differ from former collision data and the received collision data differ it adds to the collision data which received the 2nd time stamp and VIN, and it comes out with the microprocessor which generates the 2nd information, and is constituted.
[0005]
[Problem(s) to be Solved by the Invention] However, if it is in the above-mentioned conventional car control event data authentication equipment, in order to generate a time stamp based on the value acquired from the internal timer and to add this to control event information, the value of an internal timer might be changed by the user, or the value of an internal timer might shift according to causes, such as long term deterioration, and there was a problem that the certification force as a proof of control event information was inadequate.
[0006] Moreover, the control event information recorded by the microcontroller Although a time stamp and a predetermined discernment value are included in order to guarantee that the control event information which a "sign" is added by the microcontroller, namely, was recorded was generated during operation of a specific car Since this "sign" is what is uniquely generated and added inside, it is lacking in objectivity and this also has the inadequate certification force as a proof.
[0007] Moreover, since personal ID and a vehicle identification number VIN are stored in memory in the condition as it is, it may be altered by the user and this also has the inadequate certification force as a proof.
[0008] On the other hand, the need of improving the certification force as a proof of data is considered also when as follows, a trial and.
[0009] For example, although it is possible to record the data proving who inspected when and where when inspecting in a hospital etc., since such data are data important for a patient, they are altered by nobody, but to have objectivity is desired. Therefore, there is the need of improving the certification force as a proof of data, in this case.
[0010] Moreover, although it is possible to record the data proving who followed and delivered what kind of the root when for example, when delivering a load by parcel delivery service etc., to be altered by nobody but to have objectivity, since it is required data when a load lost and damages such data in a delivery process is desired. Therefore, there is the need of improving the certification force as a proof of data, in this case.
[0011] When the photograph of an accident site and an entertainer's scoop photograph are taken, a photography person, a photography day, or a photography location is proved as a case of others, and it records investigation data by an academic investigation etc., the order of goods or service is received by the telephone, FAX, etc., order contents are specified with the other party, and composition etc. is carried out, the time of proving the generating day of copyright etc. is mentioned.
[0012] Then, this invention is made paying attention to the unsolved technical problem which such a Prior art has, and aims at offering suitable information authentication equipment and a suitable certificate authority improving the certification force as a proof of data by securing the objectivity of data.
[0013]
[Means for Solving the Problem] The information authentication equipment according to claim 1 which applies to this invention in order to attain the above-mentioned purpose is equipment which attests data, and is equipped with an authentication information addition means add to the data which generated the authentication information for attesting having inputted data as a data input means input data, with said data input means based on the information acquired from the exterior, and inputted this with said data input means.
[0014] If data are inputted with a data input means with such a configuration, the authentication information by which information was acquired from the exterior, and authentication information was generated and generated with the authentication information addition means based on the acquired information will be added to the data inputted with the data input means.
[0015] Here, all available data are contained in data on information processors, such as image data, voice and music data, document data, a data point, and other computers. Hereafter, in information authentication equipment according to claim 3, it is the same.

[0016] Moreover, as long as an authentication information addition means generates authentication information based on the information acquired from the exterior, it may be what kind of thing. For example, a time-of-day signal is received from the circumference satellite which transmits the time-of-day signal which shows current time of day. Generate the hour entry for specifying the time of inputting data with a data input means based on the received time-of-day signal as authentication information, and A time-of-day signal is received from two or more circumference satellites, and the positional information for pinpointing the point which inputted data with the data input means based on a gap of the time of day shown by these time-of-day signal and the circumference orbit of each circumference satellite is generated as authentication information. Moreover, when generating a hour entry like the former, a time-of-day signal may be received from an electric-wave clock (what is being sent at the Ministry of Posts and Telecommunications).
[0017] Furthermore, the information authentication equipment according to claim 2 concerning this invention In information authentication equipment according to claim 1 said authentication information addition means It has a location measurement means to measure a location using an external information dispatch means, and the positional information for pinpointing the point which inputted data with said data input means based on the location measured with said location measurement means is generated, and the generated positional information is added as authentication information.
[0018] With such a configuration, a location is measured by the location measurement means using an external information dispatch means, positional information is generated by the authentication information addition means based on the location measured with the location measurement means, and the generated positional information is added as authentication information.
[0019] Here, as an external information dispatch means, the cellular phone based on PHS (Personal Handyphone System), GSM (Global System for Mobile Communication), or IMT-2000 or GPS (Global Positioning System) is mentioned.
[0020] Moreover, the information authentication equipment according to claim 3 concerning this invention A data input means to be equipment which attests data using the certificate authority which performs a digital signature, and to input data, It has an authentication information addition means to add the authentication information for attesting having inputted data with said data input means to the data inputted with said data input means, and a transmitting means to transmit the data which added authentication information with said authentication information addition means to said certificate authority.
[0021] If data are inputted with a data input means with such a configuration, the data to which authentication information was added to the data inputted with the data input means by the authentication information addition means, and authentication information was added with the authentication information addition means by the transmitting means will be transmitted to a certificate authority. And a digital signature is performed by the certificate authority to the data transmitted from information authentication equipment.
[0022] Information authentication equipment operates how here, after transmitting data to a certificate authority. For example, receive the data which performed the digital signature from a certificate authority, memorize the received data, and The data which performed the digital signature are made to hold to a certificate authority, and the data which performed the digital signature are transmitted to other terminals through a certificate authority.
[0023] Furthermore, in information authentication equipment according to claim 3, said authentication information addition means has a timing measurement means measure time amount, and the information authentication equipment according to claim 4 concerning this invention generates the hour entry for specifying the time of inputting data with said data input means based on the time amount measured with said timing measurement means, and adds the generated hour entry as authentication information.
[0024] With such a configuration, time amount is measured by the timing measurement means, a hour entry is generated by the authentication information addition means based on the time amount measured with the timing measurement means, and the generated hour entry is added as authentication information.
[0025] Here, as long as a timing measurement means measures time amount, it may be what kind of thing, for example, it measures the time amount which has passed since the base period, and measures current time of day. Moreover, a circumference satellite is used, time amount is measured using the information acquired from the exterior, a clock timer is built in and time amount is measured using the information generated inside.
[0026] Furthermore, said authentication information addition means has a location measurement means measure a location, and the information authentication equipment according to claim 5 concerning this invention generates the positional information for pinpointing the point which inputted data with said data input means based on the location which measured with said location measurement means, and adds the positional information which generated as authentication information in information authentication equipment given in either of claims 3 and 4.
[0027] With such a configuration, a location is measured by the location measurement means, positional information is generated by the authentication information addition means based on the location measured with the location measurement means, and the generated positional information is added as authentication information.
[0028] Here, as long as a location measurement means measures a location, it may be what kind of thing, for example, it uses GPS, measures a location using the information acquired from the exterior, uses a gyroscope and an accelerometer, and measures a location using the information generated inside.
[0029] Furthermore, the information authentication equipment according to claim 6 concerning this invention In information authentication equipment according to claim 3 to 5 said authentication information addition means Have an environment condition measurement means to measure a surrounding environment condition, and it is based on the environment condition measured with said environment condition measurement means. The environment condition information for specifying the environment condition at the time of inputting data with said data input means is generated, and the generated environment condition information is added as authentication information.
[0030] With such a configuration, a surrounding environment condition is measured by the environment condition measurement means, environment condition information is generated by the authentication information addition means based on the environment condition measured with the environment condition measurement means, and the generated environment condition information is added as authentication information.
[0031] Here, if a surrounding environment condition is measured, an environment condition measurement means may be what kind of thing, for example, should just measure temperature, humidity, an atmospheric pressure, gas concentration, a wind speed, the altitude, surrounding sound volume, or the surrounding quantity of light.
[0032] Furthermore, the information authentication equipment according to claim 7 concerning this invention The individual humanity news storage means for memorizing individual humanity news in information authentication equipment according to claim 3 to 6, It has an individual humanity news input means to input individual humanity news. Said authentication information addition means While the individual

humanity news inputted with said individual humanity news input means and the individual humanity news of said individual humanity news storage means are filling predetermined relation, the individual humanity news of said individual humanity news storage means is added as authentication information.

[0033] If individual humanity news is inputted with an individual humanity news input means, while the individual humanity news and the individual humanity news of an individual humanity news storage means which were inputted are filling predetermined relation with such a configuration, the individual humanity news of an individual humanity news storage means is added as authentication information.

[0034] Here, the information depending on the living environment of individuals, such as information for which it depended on the description of the body of individuals, such as the ID code and blood group which were assigned for every individual, and a fingerprint, as individual humanity news, for example or the address, and the telephone number, is mentioned.

[0035] To fill predetermined relation Moreover, for example, the thing the individual humanity news for collating and the individual humanity news for [collated] are [thing] in agreement, The result of having calculated by predetermined operation expression using the individual humanity news for collating is in agreement with the individual humanity news for [collated], Or ** with the result of having calculated by predetermined operation expression using the individual humanity news for collating, and the result in agreement of having calculated by predetermined operation expression using the individual humanity news for [collated] is mentioned.

[0036] Moreover, an individual humanity news storage means is every means, and may memorize individual humanity news at all stages, and may memorize individual humanity news beforehand, and you may make it memorize individual humanity news at the time of actuation of this equipment.

[0037] Furthermore, the information authentication equipment according to claim 8 concerning this invention equips the information authentication equipment concerned with the equipment information storage means for memorizing the equipment information which is the information on a proper in information authentication equipment according to claim 3 to 7, and said authentication information addition means adds the equipment information on said equipment information storage means as authentication information.

[0038] With such a configuration, the equipment information on an equipment information storage means is added as authentication information by the authentication information addition means.

[0039] An equipment information storage means is every means, and may memorize equipment information at all stages, and may memorize equipment information beforehand, and you may make it memorize equipment information here at the time of actuation of this equipment.

[0040] Furthermore, in information authentication equipment according to claim 3 to 8, said authentication information addition means generates the inspection information for inspecting whether the error is contained in the data concerned using the data inputted with said data input means, and the information authentication equipment according to claim 9 concerning this invention adds the generated inspection information as authentication information.

[0041] With such a configuration, the inspection information by which inspection information was generated and generated with the authentication information addition means using the data inputted with the data input means is added as authentication information.

[0042] the information for inspecting whether the error is contained in data with inspection information here -- saying -- as such information -- a parity check code and a group -- counting -- error correcting codes, such as error detecting codes, such as a check code, and CRC (cyclic redundancy check), Hamming code, the inspection information for conducting limit check and sum check, and the encryption information that enciphered data by the predetermined code key can be mentioned. In the following and a certificate authority according to claim 18, it is the same.

[0043] Furthermore, a Hash Function generates inspection information using the data into which the information authentication equipment according to claim 10 concerning this invention inputted said authentication information addition means with said data input means in information authentication equipment according to claim 9.

[0044] With such a configuration, inspection information is generated by the Hash Function using the data inputted with the data input means by the authentication information addition means.

[0045] Furthermore, the information authentication equipment according to claim 11 concerning this invention enciphers the data with which said authentication information addition means added authentication information in information authentication equipment according to claim 3 to 10.

[0046] With such a configuration, the data with which authentication information was added are enciphered by the authentication information addition means. And the enciphered data are transmitted to a certificate authority by the transmitting means.

[0047] Here, a cipher system may be what kind of thing, for example, may be a common key encryptosystem-ized method, and may be a public-key-encryption-ized method. As these cipher systems, for example as a block cipher system, the cipher system of a exponentiation and remainder molds, such as a cipher system of stirring / permutation molds, such as DES (Data Encryption Standard), RC5, and FEAL, or RSA, an ElGamal cryptosystem, a DH process, and a elliptic curve cryptosystem, is held, and RC4, the Barnum code, NLFSR, etc. are mentioned as a stream cipher-ized method.

[0048] Furthermore, in information authentication equipment according to claim 11, said cipher system of the information authentication equipment according to claim 12 concerning this invention is a public-key-encryption-ized method, and said authentication information addition means enciphers the data which added authentication information with the private key of the information authentication equipment concerned.

[0049] With such a configuration, the data with which authentication information was added are enciphered with the private key of the information authentication equipment by the authentication information addition means.

[0050] Furthermore, the information authentication equipment according to claim 13 concerning this invention is equipped with a receiving means to receive the data with which the digital signature was added by said certificate authority from the certificate authority concerned, and a data storage means to memorize the data which received with said receiving means, in information authentication equipment according to claim 3 to 12.

[0051] With such a configuration, the data to which it was transmitted by the receiving means with the transmitting means, and the digital signature was added by the certificate authority by it are received from the certificate authority, and the received data are memorized by the data storage means.

[0052] On the other hand, in order to attain the above-mentioned purpose, the certificate authority according to claim 14 concerning this invention A certificate authority side receiving means to be the certificate authority which performs a digital signature to the data transmitted from information authentication equipment according to claim 3 to 13, and to receive data from said information authentication equipment, It has a digital signature addition means to add a digital signature to the data received with said certificate authority side

receiving means. Said digital signature addition means When it attests having inputted data with said data input means based on the authentication information added to the data received with said certificate authority side receiving means, a digital signature is added to the data received with said certificate authority side receiving means.

[0053] When it was such a configuration, and data were received by the certificate authority side receiving means from information authentication equipment and having inputted data with the data input means with the digital signature addition means based on the authentication information added to the data received with the certificate authority side receiving means is attested, a digital signature is added to the data received with the certificate authority side receiving means.

[0054] Furthermore, the certificate authority according to claim 15 concerning this invention In a certificate authority according to claim 14 said digital signature addition means While the time amount specified by the hour entry added as authentication information on the data which have a certificate authority side timing measurement means to measure time amount, and were received with said certificate authority side receiving means, and the time amount measured with said certificate authority side timing measurement means are filling predetermined relation A digital signature is added to the data received with said certificate authority side receiving means.

[0055] With such a configuration, time amount is measured by the certificate authority side timing measurement means, and while the time amount specified by the hour entry added as authentication information on the data received with the certificate authority side receiving means by the digital signature addition means and the time amount measured with the certificate authority side timing measurement means are filling predetermined relation, a digital signature is added to the data received with the certificate authority side receiving means.

[0056] Here, as long as a certificate authority side timing measurement means measures time amount, it may be what kind of thing, for example, it may measure the time amount which has passed since the base period, and may measure current time of day. Moreover, a circumference satellite is used, time amount is measured using the information acquired from the exterior, a clock timer is built in and time amount is measured using the information generated inside.

[0057] Moreover, the time amount for example, for collating and the time amount for [collated] being in agreement and being [the time difference of the time amount for collating and the time amount for / collated / predetermined within the limits] ** are mentioned to filling predetermined relation.

[0058] Furthermore, the certificate authority according to claim 16 concerning this invention In a certificate authority given in either of claims 14 and 15 said digital signature addition means While the location pinpointed by the positional information added as authentication information on the data which have a certificate authority side location measurement means to measure the location of said information authentication equipment, and were received with said certificate authority side receiving means, and the location measured with said certificate authority side location measurement means are filling predetermined relation A digital signature is added to the data received with said certificate authority side receiving means.

[0059] With such a configuration, the location of information authentication equipment is measured by the certificate authority side location measurement means, and while the location pinpointed by the positional information added as authentication information on the data received with a certificate authority side receiving means by the digital signature addition means and the location which were measured with a certificate authority side location measurement means are filling predetermined relation, a digital signature is added to the data received with a certificate authority side receiving means.

[0060] By being what kind of thing here, as long as a certificate authority side location measurement means measures the location of information authentication equipment, for example, communicating with the location measurement means of information authentication equipment It may be made to measure the location of information authentication equipment directly, and when information authentication equipment transmits data using a cellular phone, PHS, etc., you may make it measure the location of information authentication equipment indirectly by pinpointing the base station where information authentication equipment is communicating.

[0061] Moreover, that the location for example, for collating and the location for [collated] are in agreement, the location for [collated] being included in a predetermined field centering on the location for collating, and including [in a predetermined field / the location for collating]-centering on location for [collated] ** are mentioned to filling predetermined relation.

[0062] Furthermore, the certificate authority according to claim 17 concerning this invention Said information authentication equipment is equipped with the certificate authority side equipment information storage means for memorizing the equipment information which is the information on a proper in a certificate authority according to claim 14 to 16. While the equipment information added as authentication information on the data received with said certificate authority side receiving means and the equipment information on said certificate authority side equipment information storage means are filling predetermined relation, said digital signature addition means A digital signature is added to the data received with said certificate authority side receiving means.

[0063] While the equipment information added by the digital signature addition means as authentication information on the data received with the certificate authority side receiving means and the equipment information on a certificate authority side equipment information storage means are filling predetermined relation with such a configuration, a digital signature is added to the data received with the certificate authority side receiving means.

[0064] Here to fill predetermined relation For example, the thing the equipment information for collating and the equipment information for [collated] are [thing] in agreement, The result of having calculated by predetermined operation expression using the equipment information for collating is in agreement with the equipment information for [collated], Or ** with the result of having calculated by predetermined operation expression using the equipment information for collating, and the result in agreement of having calculated by predetermined operation expression using the equipment information for [collated] is mentioned.

[0065] Moreover, a certificate authority side equipment information storage means is every means, and may memorize equipment information at all stages, and may memorize equipment information beforehand, and you may make it memorize equipment information at the time of actuation of this equipment.

[0066] Furthermore, the certificate authority according to claim 18 concerning this invention In a certificate authority according to claim 14 to 17 said digital signature addition means The same method as information authentication equipment according to claim 9 generates inspection information using the data received with said certificate authority side receiving means. While the generated inspection information and the inspection information added as authentication information on the data received with said certificate authority side receiving means are filling predetermined relation, a digital signature is added to the data received with said certificate authority side receiving means.

[0067] With such a configuration, the data received with the certificate authority side receiving means are used with a digital signature addition means. Inspection information is generated by the same method as information authentication equipment according to claim 9.

THIS PAGE BLANK (USPTO)

While the generated inspection information and the inspection information added as authentication information on the data received with the certificate authority side receiving means are filling predetermined relation, a digital signature is added to the data received with the certificate authority side receiving means.

[0068] Here to fill predetermined relation For example, the thing the inspection information for collating and the inspection information for [collated] are [thing] in agreement, The result of having calculated by predetermined operation expression using the inspection information for collating is in agreement with the inspection information for [collated], Or ** with the result of having calculated by predetermined operation expression using the inspection information for collating, and the result in agreement of having calculated by predetermined operation expression using the inspection information for [collated] is mentioned.

[0069] Furthermore, the certificate authority according to claim 19 concerning this invention generates inspection information in a certificate authority according to claim 18 using the data which received said digital signature addition means with said certificate authority side receiving means by the same Hash Function as information authentication equipment according to claim 10.

[0070] With such a configuration, inspection information is generated by the same Hash Function as information authentication equipment according to claim 10 using the data received with the certificate authority side receiving means by the digital signature addition means.

[0071] Furthermore, the data to which the certificate authority according to claim 20 concerning this invention received said digital signature addition means with said certificate authority side receiving means in the certificate authority according to claim 14 to 19 with the cipher system of information authentication equipment according to claim 11 and the corresponding decryption method are decrypted.

[0072] With such a configuration, the data received with the certificate authority side receiving means by the cipher system of information authentication equipment according to claim 11 and the corresponding decryption method are decrypted by the digital signature addition means.

[0073] Here, a decryption method may be what kind of thing, for example, may be a common key decryption method, and may be a public key decryption method. As these decryption methods, the thing corresponding to the cipher system illustrated by the item of above-mentioned claim 11 is mentioned, for example.

[0074] Furthermore, in a certificate authority according to claim 20, said decryption method of the certificate authority according to claim 21 concerning this invention is a public key decryption method, and said digital signature addition means decrypts the data received with said certificate authority side receiving means with the public key of the information authentication equipment which is the transmitting origin of the data concerned.

[0075] With such a configuration, the data received with the certificate authority side receiving means are decrypted by the digital signature addition means with the public key of the information authentication equipment which is the transmitting origin of the data.

[0076] Furthermore, the certificate authority according to claim 22 concerning this invention is equipped with a certificate authority side transmitting means to transmit the data which added the digital signature with said digital signature addition means to said information authentication equipment, in a certificate authority according to claim 14 to 21.

[0077] With such a configuration, the data to which the digital signature was added with the digital signature addition means are transmitted to information authentication equipment by the certificate authority side transmitting means.

[0078] Furthermore, the certificate authority according to claim 23 concerning this invention is equipped with a certificate authority side data storage means to memorize the data which added the digital signature with said digital signature addition means, in a certificate authority according to claim 14 to 21.

[0079] With such a configuration, the data to which the digital signature was added with the digital signature addition means are memorized by the certificate authority side data storage means.

[0080] Although the information authentication equipment and the certificate authority for attaining the above-mentioned purpose were proposed above, since not only this but the above-mentioned purpose is attained, the following information authentication system can also be proposed.

[0081] This information authentication system is a system which connected the certificate authority which performs a digital signature, and information authentication equipment possible [a communication link] through the network. Said information authentication equipment A data input means to input data, and an individual humanity news input means to input individual humanity news, The individual humanity news storage means for memorizing individual humanity news, and the equipment information storage means for memorizing the equipment information which is the information on a proper to the information authentication equipment concerned, An authentication information addition means to add the authentication information for attesting having inputted data with said data input means to the data inputted with said data input means, It has a transmitting means to transmit the data which added authentication information with said authentication information addition means to said certificate authority. Said authentication information addition means A timing measurement means to measure time amount, a location measurement means to measure a location, and an environment condition measurement means to measure a surrounding environment condition, A hour entry generation means to generate the hour entry for specifying the time of inputting data with said data input means based on the time amount measured with said timing measurement means, A positional information generation means to generate the positional information for pinpointing the point which inputted data with said data input means based on the location measured with said location measurement means, An environment condition information generation means to generate the environment condition information for specifying the environment condition at the time of inputting data with said data input means based on the environment condition measured with said environment condition measurement means, An inspection information generation means to generate the inspection information for inspecting whether the error is contained in the data concerned using the data inputted with said data input means, While the individual humanity news which it ****(ed) and was inputted with said individual humanity news input means, and the individual humanity news of said individual humanity news storage means are filling predetermined relation The equipment information on said equipment information storage means and the individual humanity news of said individual humanity news storage means are added for the generated hour entry, positional information, environment condition information, and inspection information to a list as authentication information. A certificate authority side receiving means by which said certificate authority receives data from said information authentication equipment, The certificate authority side equipment information storage means for memorizing the equipment information which is the information on a proper to said information authentication equipment, It has a digital signature addition means to add a digital signature to the data received with said certificate authority side receiving means. Said digital signature addition means A certificate authority side timing measurement means to measure time amount, and a certificate authority side location measurement means to measure the location of said information authentication equipment, A certificate authority side inspection information generation means to generate inspection information with the same method as said inspection information generation means

using the data received with said certificate authority side receiving means,

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is the block diagram showing the configuration of an information authentication system.
[Drawing 2] It is the block diagram showing the configuration of an information processor 40.
[Drawing 3] It is the flow chart which shows authentication information attached processing.
[Drawing 4] It is the block diagram showing the configuration of an information processor 50.
[Drawing 5] It is the flow chart which shows digital signature attached processing.
[Description of Notations]
100 Information Authentication Equipment
120 Authentication Information Adjunct
200 Certificate Authority
220 Digital Office Naming Kabe
10 Digital Camera
12 26 Individual humanity news input unit
14 Individual Humanity News Storage
16 28 Equipment information storage device
18 24 Communication device
20 Data Storage
40 50 Information processor
42 52 Timing measurement equipment
44 54 Location measuring device
S1-Sn Sensor
46 User Authentication Equipment
60,70 CPU
62,72 ROM
64,74 RAM

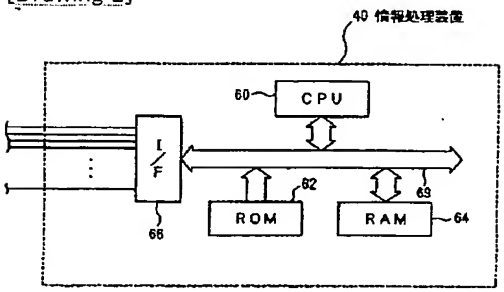
[Translation done.]

* NOTICES *

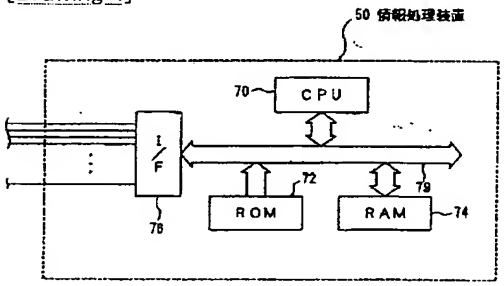
1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

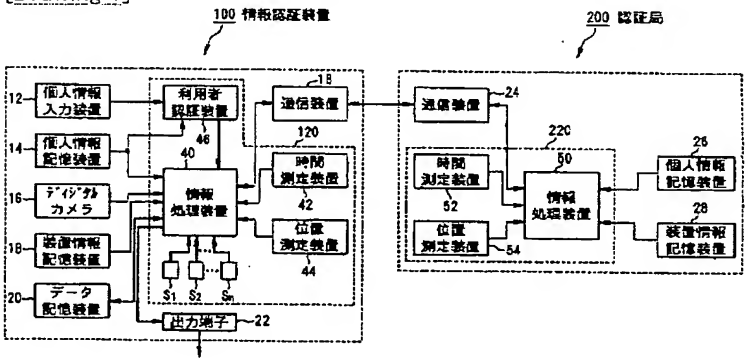
[Drawing 2]



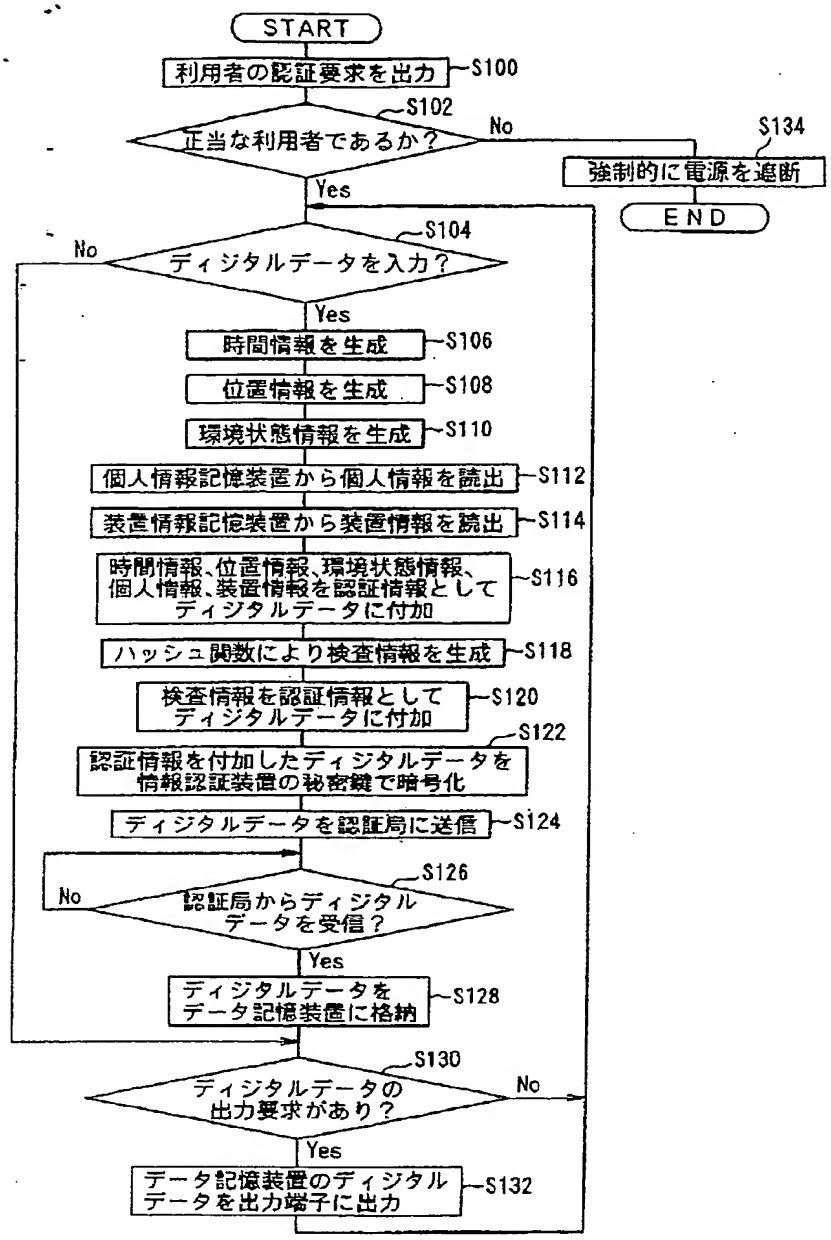
[Drawing 4]



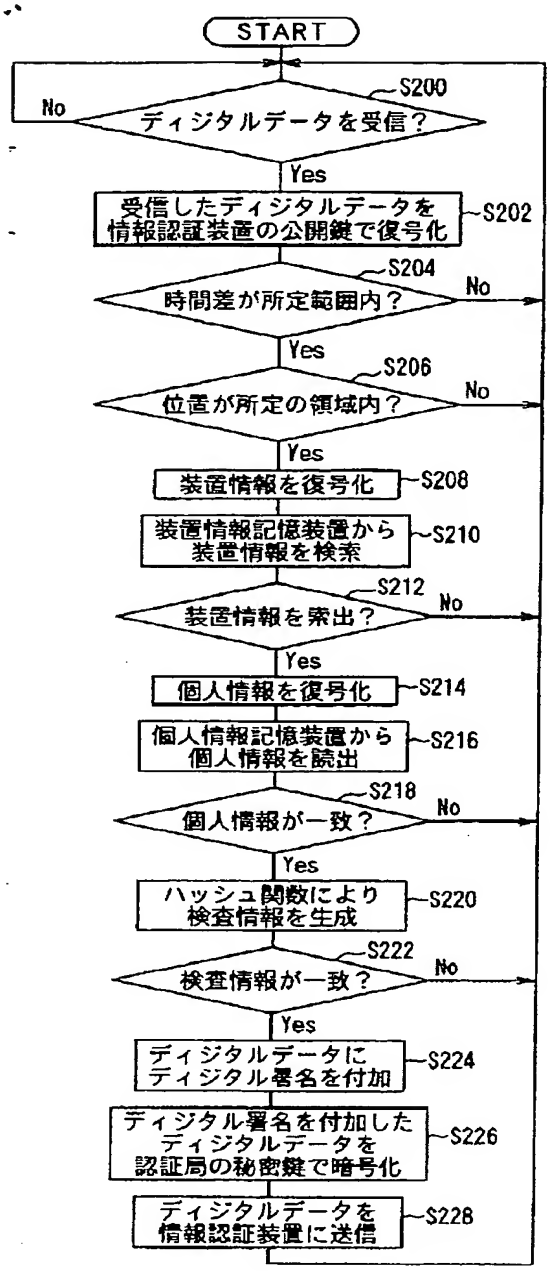
[Drawing 1]



[Drawing 3]


START
利用者の認証要求を出力
S100
S102
正当な利用者であるか？
No
S134
強制的に電源を遮断
END
Yes
S104
No
ディジタルデータを入力？
Yes
時間情報を生成
S106
位置情報を生成
S108
環境状態情報を生成
S110
個人情報記憶装置から個人情報を読出
S112
装置情報記憶装置から装置情報を読出
S114
時間情報、位置情報、環境状態情報、
個人情報、装置情報を認証情報として
ディジタルデータに付加
S116
ハッシュ関数により検査情報を生成
S118
検査情報を認証情報として
ディジタルデータに付加
S120
S122
認証情報を付加したディジタルデータを
情報認証装置の秘密鍵で暗号化
ディジタルデータを認証局に送信
S124
S126
No
認証局からディジタル
データを受信？
Yes
ディジタルデータを
データ記憶装置に格納
S128
S130
ディジタルデータの
出力要求があり？
No
Yes
データ記憶装置のディジタル
データを出力端子に出力
S132

[Drawing 5]



[Translation done.]

* NOTICES *

CORRECTION OR AMENDMENT

[Kind of official gazette] Printing of amendment by the convention of 2 of Article 17 of Patent Law
[Section partition] The 2nd partition of the 6th section
[Publication date] February 24, Heisei 17 (2005. 2.24)

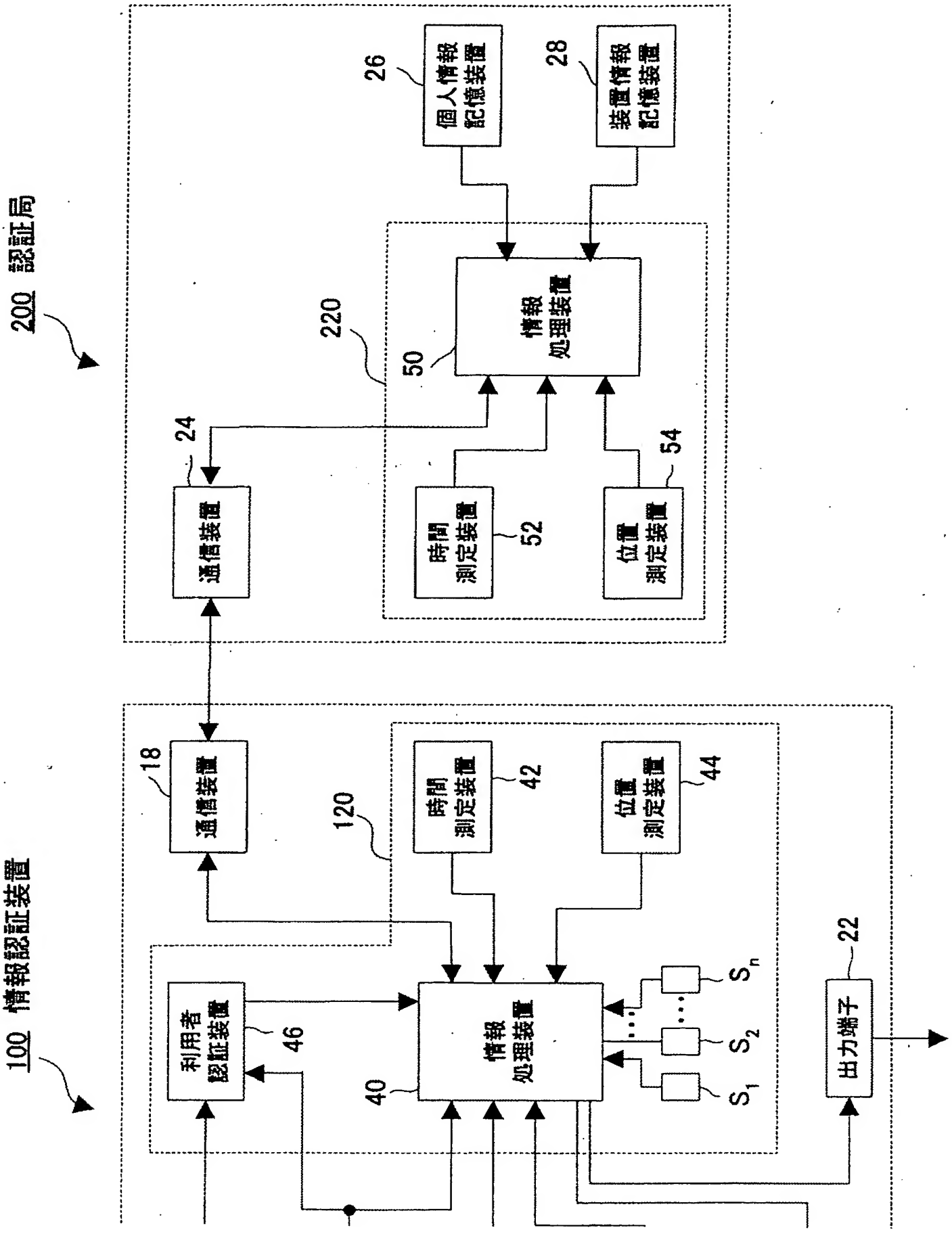
[Publication No.] JP,2001-100632,A (P2001-100632A)
[Date of Publication] April 13, Heisei 13 (2001. 4.13)
[Application number] Japanese Patent Application No. 11-280825
[The 7th edition of International Patent Classification]

G09C 1/00
G09C 5/00
H04L 9/32

[FI]

G09C 1/00 640 B
G09C 1/00 640 Z
G09C 5/00
H04L 9/00 675 D
H04L 9/00 675 B

[Procedure revision]
[Filing Date] March 18, Heisei 16 (2004. 3.18)
[Procedure amendment 1]
[Document to be Amended] DRAWINGS
[Item(s) to be Amended] drawing 1
[Method of Amendment] Modification
[The contents of amendment]
[Drawing 1]


100 情報認証装置
200 認証局
18 通信装置
120
時間測定装置 42
位置測定装置 44
利用者認証装置 46
40 情報処理装置
S_1 S_2 S_n
22 出力端子
24 通信装置
220
50 情報処理装置
26 個人情報記憶装置
28 装置情報記憶装置
時間測定装置 52
位置測定装置 54

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2001－100632
（P2001－100632A）
(43)公開日　平成13年４月13日(2001.4.13)

(51)Int.Cl.⁷		識別記号	FI		テーマコード（参考）
G09C	1/00	640	G09C	1/00	640B　5J104
					640Z
	5/00			5/00	
H04L	9/32		H04L	9/00	675D
					675B

審査請求　未請求　請求項の数23　ＯＬ　（全 21 頁）

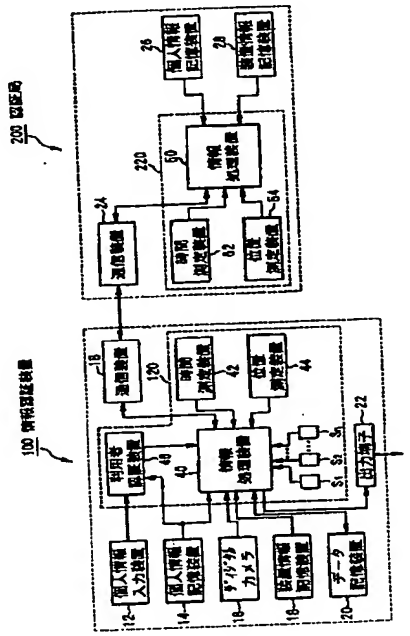
(21)出願番号　特願平11－280825
(22)出願日　平成11年９月30日(1999.9.30)

(71)出願人　000002369
セイコーエプソン株式会社
東京都新宿区西新宿２丁目４番１号
(72)発明者　小林　道夫
長野県諏訪市大和３丁目３番５号　セイコーエプソン株式会社内
(74)代理人　100093388
弁理士　鈴木　喜三郎　（外２名）

Ｆターム(参考)　5J104 AA07 AA09 AA11 AA14 EA03
KA01 LA03 LA06 MA02 NA02
NA05 NA12 NA36 NA37 NA38
PA07

(54)【発明の名称】　情報認証装置及び認証局

(57)【要約】
【課題】　データの客観性を確保することにより、データの証拠としての証明力を向上するのに好適な情報認証装置および認証局を提供する。
【解決装置】　情報認証装置１００は、ディジタルカメラ１０と、ディジタルカメラ１０で入力したディジタルデータに認証情報を付加する認証情報付加部１２０と、で構成されている。一方、認証局２００は、情報認証装置１００からディジタルデータを受信する通信装置２４と、ディジタル署名付加部２２０と、を備え、ディジタル署名付加部２２０は、通信装置２４で受信したディジタルデータに付加された認証情報に基づいて、ディジタルカメラ１０でディジタルデータを入力したことを認証したときは、通信装置２４で受信したディジタルデータにディジタル署名を付加するようになっている。



1

【特許請求の範囲】

【請求項１】　データの認証を行う装置であって、
データを入力するデータ入力手段と、外部から取得した情報に基づいて前記データ入力手段でデータを入力したことを認証するための認証情報を生成してこれを前記データ入力手段で入力したデータに付加する認証情報付加手段と、を備えることを特徴とする情報認証装置。

【請求項２】　請求項１において、
前記認証情報付加手段は、外部情報発信手段を利用して位置を測定する位置測定手段を有し、前記位置測定手段で測定した位置に基づいて、前記データ入力手段でデータを入力した地点を特定するための位置情報を生成し、生成した位置情報を認証情報として付加するようになっていることを特徴とする情報認証装置。

【請求項３】　ディジタル署名を行う認証局を利用してデータの認証を行う装置であって、
データを入力するデータ入力手段と、前記データ入力手段でデータを入力したことを認証するための認証情報を前記データ入力手段で入力したデータに付加する認証情報付加手段と、前記認証情報付加手段で認証情報を付加したデータを前記認証局に送信する送信手段と、を備えることを特徴とする情報認証装置。

【請求項４】　請求項３において、
前記認証情報付加手段は、時間を測定する時間測定手段を有し、前記時間測定手段で測定した時間に基づいて、前記データ入力手段でデータを入力した時点を特定するための時間情報を生成し、生成した時間情報を認証情報として付加するようになっていることを特徴とする情報認証装置。

【請求項５】　請求項３及び４のいずれかにおいて、
前記認証情報付加手段は、位置を測定する位置測定手段を有し、前記位置測定手段で測定した位置に基づいて、前記データ入力手段でデータを入力した地点を特定するための位置情報を生成し、生成した位置情報を認証情報として付加するようになっていることを特徴とする情報認証装置。

【請求項６】　請求項３乃至５のいずれかにおいて、
前記認証情報付加手段は、周囲の環境状態を測定する環境状態測定手段を有し、前記環境状態測定手段で測定した環境状態に基づいて、前記データ入力手段でデータを入力した時点における環境状態を特定するための環境状態情報を生成し、生成した環境状態情報を認証情報として付加するようになっていることを特徴とする情報認証装置。

【請求項７】　請求項３乃至６のいずれかにおいて、
個人情報を記憶するための個人情報記憶手段と、個人情報を入力する個人情報入力手段と、を備え、
前記認証情報付加手段は、前記個人情報入力手段で入力した個人情報と前記個人情報記憶手段の個人情報とが所定関係を満たしているときは、前記個人情報記憶手段の

2

個人情報を認証情報として付加するようになっていることを特徴とする情報認証装置。

【請求項８】　請求項３乃至７のいずれかにおいて、
当該情報認証装置に固有の情報である装置情報を記憶するための装置情報記憶手段を備え、
前記認証情報付加手段は、前記装置情報記憶手段の装置情報を認証情報として付加するようになっていることを特徴とする情報認証装置。

【請求項９】　請求項３乃至８のいずれかにおいて、
前記認証情報付加手段は、前記データ入力手段で入力したデータを用いて、当該データに誤りが含まれているか否かを検査するための検査情報を生成し、生成した検査情報を認証情報として付加するようになっていることを特徴とする情報認証装置。

【請求項１０】　請求項９において、
前記認証情報付加手段は、前記データ入力手段で入力したデータを用いて、ハッシュ関数により検査情報を生成するようになっていることを特徴とする情報認証装置。

【請求項１１】　請求項３乃至１０のいずれかにおいて、
前記認証情報付加手段は、認証情報を付加したデータを暗号化するようになっていることを特徴とする情報認証装置。

【請求項１２】　請求項１１において、
前記暗号化方式は、公開鍵暗号化方式であり、
前記認証情報付加手段は、認証情報を付加したデータを当該情報認証装置の秘密鍵で暗号化するようになっていることを特徴とする情報認証装置。

【請求項１３】　請求項３乃至１２のいずれかにおいて、
前記認証局でディジタル署名が付加されたデータを当該認証局から受信する受信手段と、前記受信手段で受信したデータを記憶するデータ記憶手段と、を備えることを特徴とする情報認証装置。

【請求項１４】　請求項３乃至１３のいずれかに記載の情報認証装置から送信されたデータに対してディジタル署名を行う認証局であって、
前記情報認証装置からデータを受信する認証局側受信手段と、前記認証局側受信手段で受信したデータにディジタル署名を付加するディジタル署名付加手段と、を備え、
前記ディジタル署名付加手段は、前記認証局側受信手段で受信したデータに付加された認証情報に基づいて、前記データ入力手段でデータを入力したことを認証したときは、前記認証局側受信手段で受信したデータにディジタル署名を付加するようになっていることを特徴とする認証局。

【請求項１５】　請求項１４において、
前記ディジタル署名付加手段は、時間を測定する認証局側時間測定手段を有し、前記認証局側受信手段で受信し

たデータの認証情報として付加された時間情報により特定される時間と前記認証局側時間測定手段で測定した時間とが所定関係を満たしているときは、前記認証局側受信手段で受信したデータにディジタル署名を付加するようになっていることを特徴とする認証局。

【請求項１６】　請求項１４及び１５のいずれかにおいて、

前記ディジタル署名付加手段は、前記情報認証装置の位置を測定する認証局側位置測定手段を有し、前記認証局側受信手段で受信したデータの認証情報として付加された位置情報により特定される位置と前記認証局側位置測定手段で測定した位置とが所定関係を満たしているときは、前記認証局側受信手段で受信したデータにディジタル署名を付加するようになっていることを特徴とする認証局。

【請求項１７】　請求項１４乃至１６のいずれかにおいて、

前記情報認証装置に固有の情報である装置情報を記憶するための認証局側装置情報記憶手段を備え、

前記ディジタル署名付加手段は、前記認証局側受信手段で受信したデータの認証情報として付加された装置情報と前記認証局側装置情報記憶手段の装置情報とが所定関係を満たしているときは、前記認証局側受信手段で受信したデータにディジタル署名を付加するようになっていることを特徴とする認証局。

【請求項１８】　請求項１４乃至１７のいずれかにおいて、

前記ディジタル署名付加手段は、前記認証局側受信手段で受信したデータを用いて、請求項９記載の情報認証装置と同一の方式により検査情報を生成し、生成した検査情報と前記認証局側受信手段で受信したデータの認証情報として付加された検査情報とが所定関係を満たしているときは、前記認証局側受信手段で受信したデータにディジタル署名を付加するようになっていることを特徴とする認証局。

【請求項１９】　請求項１８において、

前記ディジタル署名付加手段は、前記認証局側受信手段で受信したデータを用いて、請求項１０記載の情報認証装置と同一のハッシュ関数により検査情報を生成するようになっていることを特徴とする認証局。

【請求項２０】　請求項１４乃至１９のいずれかにおいて、

前記ディジタル署名付加手段は、請求項１１記載の情報認証装置の暗号化方式と対応する復号化方式により前記認証局側受信手段で受信したデータを復号化するようになっていることを特徴とする認証局。

【請求項２１】　請求項２０において、

前記復号化方式は、公開鍵復号化方式であり、

前記ディジタル署名付加手段は、前記認証局側受信手段で受信したデータを、当該データの送信元である情報認証装置の公開鍵で復号化するようになってることを特徴とする認証局。

【請求項２２】　請求項１４乃至２１のいずれかにおいて、

前記ディジタル署名付加手段でディジタル署名を付加したデータを前記情報認証装置に送信する認証局側送信手段を備えることを特徴とする認証局。

【請求項２３】　請求項１４乃至２１のいずれかにおいて、

前記ディジタル署名付加手段でディジタル署名を付加したデータを記憶する認証局側データ記憶手段を備えることを特徴とする認証局。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、データの認証を行う情報認証装置および認証局に係り、特に、データの客観性を確保することにより、データの証拠としての証明力を向上するのに好適な情報認証装置および認証局に関する。

【０００２】

【従来の技術】近年、アメリカ等では、通常のカメラで撮影した写真のほか、ディジタルカメラで撮影したディジタル画像も裁判の証拠として認められるようになってきている。しかし、ディジタル画像等のディジタルデータは、一般に改ざんが比較的容易であるため、証拠の証明力が不十分であるという問題があった。

【０００３】従来、ディジタルデータの証拠としての証明力を向上する技術に関連するものとして、例えば、特開平11-115831号公報に開示された車両制御イベントデータ認証装置がある。

【０００４】これは、車両事故の発生前、発生中または発生後に運転者によって実行された一連の運転操作等の制御イベントを記録するものであって、制御イベント情報を受信すべく結合され、第１タイム・スタンプおよび車両識別番号ＶＩＮを制御イベント情報に付加して第１情報を与え、第１情報をタイム・オーバラップ方式でメモリに出力するマイクロコントローラと、マイクロコントローラおよびマイクロプロセッサに結合され、第１情報および第２情報をタイム・オーバラップ方式で格納するメモリと、メモリおよび複数のトランスデューサに結合され、受信した衝突データが以前の衝突データとは異なるかどうかを判定し、受信した衝突データが異なるときは、第２タイム・スタンプおよびＶＩＮを受信した衝突データに追加して、第２情報を生成するマイクロプロセッサと、で構成されている。

【０００５】

【発明が解決しようとする課題】しかしながら、上記従来の車両制御イベントデータ認証装置にあっては、内部タイマから取得した値に基づいてタイム・スタンプを生成してこれを制御イベント情報に付加するようになって

いるため、内部タイマの値が利用者によって変更されたり、経年劣化等の原因により内部タイマの値がずれたりする可能性があり、制御イベント情報の証拠としての証明力が不十分であるという問題があった。

【０００６】また、マイクロコントローラによって記録される制御イベント情報は、マイクロコントローラによって「サイン」が付加される、すなわち、記録された制御イベント情報が特定の車両の運転中に生成されたことを保証するために、タイム・スタンプと所定の識別値とを含むようになっているが、この「サイン」は、内部で独自に生成・付加されるものであるため、客観性に乏しく、これも証拠としての証明力が不十分である。

【０００７】また、パーソナルＩＤや車両識別番号ＶＩＮがそのままの状態でメモリに格納されるため、利用者によって改ざんされる可能性があり、これも証拠としての証明力が不十分である。

【０００８】一方、データの証拠としての証明力を向上する必要性は、裁判だけに限らず、次のような場合にも考えられる。

【０００９】例えば、病院等で検査を行う場合には、いつ誰がどこで検査を行ったかということを証明するデータを記録しておくことが考えられるが、こうしたデータは、患者にとって重要なデータであることから、誰にも改ざんされず、客観性を有していることが望まれる。したがって、この場合は、データの証拠としての証明力を向上する必要性がある。

【００１０】また例えば、宅配便等で荷物を配送する場合には、いつ誰がどのようなルートをたどって配送したかを証明するデータを記録しておくことが考えられるが、こうしたデータは、配送過程で荷物が紛失・破損したときに必要なデータであることから、誰にも改ざんされず、客観性を有していることが望まれる。したがって、この場合は、データの証拠としての証明力を向上する必要性がある。

【００１１】その他の場合としては、事故現場の写真や芸能人のスクープ写真を撮影した場合に撮影者、撮影日または撮影場所を証明するとき、学術調査等で調査データを記録する場合、電話やＦＡＸ等で商品またはサービスの注文を受け付けた場合に相手方と注文内容を特定するとき、作曲等をした場合に著作権の発生日を証明するときなどが挙げられる。

【００１２】そこで、本発明は、このような従来の技術の有する未解決の課題に着目してなされたものであって、データの客観性を確保することにより、データの証拠としての証明力を向上するのに好適な情報認証装置および認証局を提供することを目的としている。

【００１３】

【課題を解決するための手段】上記目的を達成するために、本発明に係る請求項１記載の情報認証装置は、データの認証を行う装置であって、データを入力するデータ入力手段と、外部から取得した情報に基づいて前記データ入力手段でデータを入力したことを認証するための認証情報を生成してこれを前記データ入力手段で入力したデータに付加する認証情報付加手段と、を備える。

【００１４】このような構成であれば、データ入力手段でデータが入力されると、認証情報付加手段により、外部から情報が取得され、取得された情報に基づいて認証情報が生成され、生成された認証情報がデータ入力手段で入力されたデータに付加される。

【００１５】ここで、データには、画像データ、音声・音楽データ、文書データ、波形データ、その他コンピュータ等の情報処理装置上で利用可能なあらゆるデータが含まれる。以下、請求項３記載の情報認証装置において同じである。

【００１６】また、認証情報付加手段は、外部から取得した情報に基づいて認証情報を生成するようになっていればどのようなものであってもよく、例えば、現在の時刻を示す時刻信号を送信する周回衛星から時刻信号を受信し、受信した時刻信号に基づいて、データ入力手段でデータを入力した時点を特定するための時間情報を認証情報として生成するようになっていてもよいし、複数の周回衛星から時刻信号を受信し、それら時刻信号により示される時刻のずれおよび各周回衛星の周回軌道に基づいて、データ入力手段でデータを入力した地点を特定するための位置情報を認証情報として生成するようになっていてもよい。また、前者のように時間情報を生成する場合、電波時計（郵政省で発信しているもの）から時刻信号を受信してもよい。

【００１７】さらに、本発明に係る請求項２記載の情報認証装置は、請求項１記載の情報認証装置において、前記認証情報付加手段は、外部情報発信手段を利用して位置を測定する位置測定手段を有し、前記位置測定手段で測定した位置に基づいて、前記データ入力手段でデータを入力した地点を特定するための位置情報を生成し、生成した位置情報を認証情報として付加するようになっている。

【００１８】このような構成であれば、位置測定手段により、外部情報発信手段を利用して位置が測定され、認証情報付加手段により、位置測定手段で測定された位置に基づいて位置情報が生成され、生成された位置情報が認証情報として付加される。

【００１９】ここで、外部情報発信手段としては、ＰＨＳ（Personal Handyphone System）、ＧＳＭ（Global System for Mobile Communication）若しくはＩＭＴ－２０００に準拠した携帯電話、またはＧＰＳ（Global Positioning System）が挙げられる。

【００２０】また、本発明に係る請求項３記載の情報認証装置は、ディジタル署名を行う認証局を利用してデータの認証を行う装置であって、データを入力するデータ入力手段と、前記データ入力手段でデータを入力したこ

とを認証するための認証情報を前記データ入力手段で入力したデータに付加する認証情報付加手段と、前記認証情報付加手段で認証情報を付加したデータを前記認証局に送信する送信手段と、を備える。

【００２１】このような構成であれば、データ入力手段でデータが入力されると、認証情報付加手段により、データ入力手段で入力されたデータに認証情報が付加され、送信手段により、認証情報付加手段で認証情報が付加されたデータが認証局に送信される。そして、認証局により、情報認証装置から送信されたデータに対してディジタル署名が行われる。

【００２２】ここで、情報認証装置は、認証局にデータを送信した後はどのように動作するようになっていてもよく、例えば、ディジタル署名を行ったデータを認証局から受信し、受信したデータを記憶するようになっていてもよいし、ディジタル署名を行ったデータを認証局に保持させるようになっていてもよいし、ディジタル署名を行ったデータを認証局を経て他の端末に送信するようになっていてもよい。

【００２３】さらに、本発明に係る請求項４記載の情報認証装置は、請求項３記載の情報認証装置において、前記認証情報付加手段は、時間を測定する時間測定手段を有し、前記時間測定手段で測定した時間に基づいて、前記データ入力手段でデータを入力した時点を特定するための時間情報を生成し、生成した時間情報を認証情報として付加するようになっている。

【００２４】このような構成であれば、時間測定手段により、時間が測定され、認証情報付加手段により、時間測定手段で測定された時間に基づいて時間情報が生成され、生成された時間情報が認証情報として付加される。

【００２５】ここで、時間測定手段は、時間を測定するようになっていればどのようなものであってもよく、例えば、基準時から経過した時間を測定するようになっていてもよいし、現在の時刻を測定するようになっていてもよい。また、周回衛星を利用するなどして、外部から取得した情報により時間を測定するようになっていてもよいし、クロックタイマを内蔵するなどして、内部で生成した情報により時間を測定するようになっていてもよい。

【００２６】さらに、本発明に係る請求項５記載の情報認証装置は、請求項３および４のいずれかに記載の情報認証装置において、前記認証情報付加手段は、位置を測定する位置測定手段を有し、前記位置測定手段で測定した位置に基づいて、前記データ入力手段でデータを入力した地点を特定するための位置情報を生成し、生成した位置情報を認証情報として付加するようになっている。

【００２７】このような構成であれば、位置測定手段により、位置が測定され、認証情報付加手段により、位置測定手段で測定された位置に基づいて位置情報が生成され、生成された位置情報が認証情報として付加される。

【００２８】ここで、位置測定手段は、位置を測定するようになっていればどのようなものであってもよく、例えば、ＧＰＳを利用するなどして、外部から取得した情報により位置を測定するようになっていてもよいし、ジャイロおよび加速度計を利用するなどして、内部で生成した情報により位置を測定するようになっていてもよい。

【００２９】さらに、本発明に係る請求項６記載の情報認証装置は、請求項３ないし５のいずれかに記載の情報認証装置において、前記認証情報付加手段は、周囲の環境状態を測定する環境状態測定手段を有し、前記環境状態測定手段で測定した環境状態に基づいて、前記データ入力手段でデータを入力した時点における環境状態を特定するための環境状態情報を生成し、生成した環境状態情報を認証情報として付加するようになっている。

【００３０】このような構成であれば、環境状態測定手段により、周囲の環境状態が測定され、認証情報付加手段により、環境状態測定手段で測定された環境状態に基づいて環境状態情報が生成され、生成された環境状態情報が認証情報として付加される。

【００３１】ここで、環境状態測定手段は、周囲の環境状態を測定するようになっていればどのようなものであってもよく、例えば、周囲の温度、湿度、気圧、ガス濃度、風速、標高、音量または光量を測定するようになっていればよい。

【００３２】さらに、本発明に係る請求項７記載の情報認証装置は、請求項３ないし６のいずれかに記載の情報認証装置において、個人情報を記憶するための個人情報記憶手段と、個人情報を入力する個人情報入力手段と、を備え、前記認証情報付加手段は、前記個人情報入力手段で入力した個人情報と前記個人情報記憶手段の個人情報とが所定関係を満たしているときは、前記個人情報記憶手段の個人情報を認証情報として付加するようになっている。

【００３３】このような構成であれば、個人情報入力手段で個人情報が入力されると、入力された個人情報と個人情報記憶手段の個人情報とが所定関係を満たしているときは、個人情報記憶手段の個人情報が認証情報として付加される。

【００３４】ここで、個人情報としては、例えば、個人ごとに割り当てられたＩＤコード、血液型や指紋等の個人の人体の特徴に依存した情報、または住所や電話番号等の個人の生活環境に依存した情報が挙げられる。

【００３５】また、所定関係を満たすことには、例えば、照合対象の個人情報と被照合対象の個人情報とが一致していること、照合対象の個人情報を用いて所定演算式により演算を行った結果が被照合対象の個人情報と一致していること、または照合対象の個人情報を用いて所定演算式により演算を行った結果と被照合対象の個人情報を用いて所定演算式により演算を行った結果が一致す

ること、が挙げられる。

【００３６】また、個人情報記憶手段は、個人情報をあらゆる手段でかつあらゆる時期に記憶するものであり、あらかじめ個人情報を記憶しておいてもよいし、本装置の動作時に個人情報を記憶するようにしてもよい。

【００３７】さらに、本発明に係る請求項８記載の情報認証装置は、請求項３ないし７のいずれかに記載の情報認証装置において、当該情報認証装置に固有の情報である装置情報を記憶するための装置情報記憶手段を備え、前記認証情報付加手段は、前記装置情報記憶手段の装置情報を認証情報として付加するようになっている。

【００３８】このような構成であれば、認証情報付加手段により、装置情報記憶手段の装置情報が認証情報として付加される。

【００３９】ここで、装置情報記憶手段は、装置情報をあらゆる手段でかつあらゆる時期に記憶するものであり、あらかじめ装置情報を記憶しておいてもよいし、本装置の動作時に装置情報を記憶するようにしてもよい。

【００４０】さらに、本発明に係る請求項９記載の情報認証装置は、請求項３ないし８のいずれかに記載の情報認証装置において、前記認証情報付加手段は、前記データ入力手段で入力したデータを用いて、当該データに誤りが含まれているか否かを検査するための検査情報を生成し、生成した検査情報を認証情報として付加するようになっている。

【００４１】このような構成であれば、認証情報付加手段により、データ入力手段で入力されたデータを用いて検査情報が生成され、生成された検査情報が認証情報として付加される。

【００４２】ここで、検査情報とは、データに誤りが含まれているか否かを検査するための情報をいい、こうした情報としては、例えば、パリティチェックコード、群計数チェックコード等の誤り検出符号や、ＣＲＣ(cyclic redundancy check)、ハミングコード等の誤り訂正符号や、限度検査、合計検査を行うための検査情報や、データを所定の暗号キーで暗号化した暗号化情報を挙げることができる。以下、請求項１８記載の認証局において同じである。

【００４３】さらに、本発明に係る請求項１０記載の情報認証装置は、請求項９記載の情報認証装置において、前記認証情報付加手段は、前記データ入力手段で入力したデータを用いて、ハッシュ関数により検査情報を生成するようになっている。

【００４４】このような構成であれば、認証情報付加手段により、データ入力手段で入力されたデータを用いてハッシュ関数により検査情報が生成される。

【００４５】さらに、本発明に係る請求項１１記載の情報認証装置は、請求項３ないし１０のいずれかに記載の情報認証装置において、前記認証情報付加手段は、認証情報を付加したデータを暗号化するようになっている。

【００４６】このような構成であれば、認証情報付加手段により、認証情報が付加されたデータが暗号化される。そして、送信手段により、暗号化されたデータが認証局に送信される。

【００４７】ここで、暗号化方式は、どのようなものであってもよく、例えば、共通鍵暗号化方式であってもよいし、公開鍵暗号化方式であってもよい。これらの暗号化方式としては、例えば、ブロック暗号化方式として、ＤＥＳ（Data Encryption Standard）、ＲＣ５、ＦＥＡＬ等の攪拌・置換型の暗号化方式、またはＲＳＡ、エルガマル暗号、ＤＨ法、楕円暗号等のべき乗・剰余型の暗号化方式が挙げられ、ストリーム暗号化方式として、ＲＣ４、バーナム暗号、ＮＬＦＳＲ等が挙げられる。

【００４８】さらに、本発明に係る請求項１２記載の情報認証装置は、請求項１１記載の情報認証装置において、前記暗号化方式は、公開鍵暗号化方式であり、前記認証情報付加手段は、認証情報を付加したデータを当該情報認証装置の秘密鍵で暗号化するようになっている。

【００４９】このような構成であれば、認証情報付加手段により、認証情報が付加されたデータが、その情報認証装置の秘密鍵で暗号化される。

【００５０】さらに、本発明に係る請求項１３記載の情報認証装置は、請求項３ないし１２のいずれかに記載の情報認証装置において、前記認証局でディジタル署名が付加されたデータを当該認証局から受信する受信手段と、前記受信手段で受信したデータを記憶するデータ記憶手段と、を備える。

【００５１】このような構成であれば、受信手段により、送信手段で送信され、認証局でディジタル署名が付加されたデータがその認証局から受信され、受信されたデータがデータ記憶手段に記憶される。

【００５２】一方、上記目的を達成するために、本発明に係る請求項１４記載の認証局は、請求項３ないし１３のいずれかに記載の情報認証装置から送信されたデータに対してディジタル署名を行う認証局であって、前記情報認証装置からデータを受信する認証局側受信手段と、前記認証局側受信手段で受信したデータにディジタル署名を付加するディジタル署名付加手段と、を備え、前記ディジタル署名付加手段は、前記認証局側受信手段で受信したデータに付加された認証情報に基づいて、前記データ入力手段でデータを入力したことを認証したときは、前記認証局側受信手段で受信したデータにディジタル署名を付加するようになっている。

【００５３】このような構成であれば、認証局側受信手段により情報認証装置からデータが受信されると、ディジタル署名付加手段により、認証局側受信手段で受信されたデータに付加された認証情報に基づいて、データ入力手段でデータを入力したことが認証されたときは、認証局側受信手段で受信されたデータにディジタル署名が付加される。

【００５４】さらに、本発明に係る請求項１５記載の認証局は、請求項１４記載の認証局において、前記ディジタル署名付加手段は、時間を測定する認証局側時間測定手段を有し、前記認証局側受信手段で受信したデータの認証情報として付加された時間情報により特定される時間と前記認証局側時間測定手段で測定した時間とが所定関係を満たしているときは、前記認証局側受信手段で受信したデータにディジタル署名を付加するようになっている。

【００５５】このような構成であれば、認証局側時間測定手段により、時間が測定され、ディジタル署名付加手段により、認証局側受信手段で受信されたデータの認証情報として付加された時間情報により特定される時間と認証局側時間測定手段で測定された時間とが所定関係を満たしているときは、認証局側受信手段で受信されたデータにディジタル署名が付加される。

【００５６】ここで、認証局側時間測定手段は、時間を測定するようになっていればどのようなものであってもよく、例えば、基準時から経過した時間を測定するものであってもよいし、現在の時刻を測定するものであってもよい。また、周回衛星を利用するなどして、外部から取得した情報により時間を測定するようになっていてもよいし、クロックタイマを内蔵するなどして、内部で生成した情報により時間を測定するようになっていてもよい。

【００５７】また、所定関係を満たすことには、例えば、照合対象の時間と被照合対象の時間とが一致していること、照合対象の時間と被照合対象の時間との時間差が所定範囲内であること、が挙げられる。

【００５８】さらに、本発明に係る請求項１６記載の認証局は、請求項１４および１５のいずれかに記載の認証局において、前記ディジタル署名付加手段は、前記情報認証装置の位置を測定する認証局側位置測定手段を有し、前記認証局側受信手段で受信したデータの認証情報として付加された位置情報により特定される位置と前記認証局側位置測定手段で測定した位置とが所定関係を満たしているときは、前記認証局側受信手段で受信したデータにディジタル署名を付加するようになっている。

【００５９】このような構成であれば、認証局側位置測定手段により、情報認証装置の位置が測定され、ディジタル署名付加手段により、認証局側受信手段で受信されたデータの認証情報として付加された位置情報により特定される位置と認証局側位置測定手段で測定された位置とが所定関係を満たしているときは、認証局側受信手段で受信されたデータにディジタル署名が付加される。

【００６０】ここで、認証局側位置測定手段は、情報認証装置の位置を測定するようになっていればどのようなものであってもよく、例えば、情報認証装置の位置測定手段と通信を行うことにより、情報認証装置の位置を直接的に測定するようにしてもよいし、情報認証装置が携帯電話やＰＨＳ等を利用してデータを送信するような場合は、情報認証装置が通信している基地局を特定することにより、情報認証装置の位置を間接的に測定するようにしてもよい。

【００６１】また、所定関係を満たすことには、例えば、照合対象の位置と被照合対象の位置とが一致していること、照合対象の位置を中心として所定の領域内に被照合対象の位置が含まれていること、被照合対象の位置を中心として所定の領域内に照合対象の位置が含まれていること、が挙げられる。

【００６２】さらに、本発明に係る請求項１７記載の認証局は、請求項１４ないし１６のいずれかに記載の認証局において、前記情報認証装置に固有の情報である装置情報を記憶するための認証局側装置情報記憶手段を備え、前記ディジタル署名付加手段は、前記認証局側受信手段で受信したデータの認証情報として付加された装置情報と前記認証局側装置情報記憶手段の装置情報とが所定関係を満たしているときは、前記認証局側受信手段で受信したデータにディジタル署名を付加するようになっている。

【００６３】このような構成であれば、ディジタル署名付加手段により、認証局側受信手段で受信されたデータの認証情報として付加された装置情報と認証局側装置情報記憶手段の装置情報とが所定関係を満たしているときは、認証局側受信手段で受信されたデータにディジタル署名が付加される。

【００６４】ここで、所定関係を満たすことには、例えば、照合対象の装置情報と被照合対象の装置情報とが一致していること、照合対象の装置情報を用いて所定演算式により演算を行った結果が被照合対象の装置情報と一致していること、または照合対象の装置情報を用いて所定演算式により演算を行った結果と被照合対象の装置情報を用いて所定演算式により演算を行った結果が一致すること、が挙げられる。

【００６５】また、認証局側装置情報記憶手段は、装置情報をあらゆる手段でかつあらゆる時期に記憶するものであり、あらかじめ装置情報を記憶しておいてもよいし、本装置の動作時に装置情報を記憶するようにしてもよい。

【００６６】さらに、本発明に係る請求項１８記載の認証局は、請求項１４ないし１７のいずれかに記載の認証局において、前記ディジタル署名付加手段は、前記認証局側受信手段で受信したデータを用いて、請求項９記載の情報認証装置と同一の方式により検査情報を生成し、生成した検査情報と前記認証局側受信手段で受信したデータの認証情報として付加された検査情報とが所定関係を満たしているときは、前記認証局側受信手段で受信したデータにディジタル署名を付加するようになっている。

【００６７】このような構成であれば、ディジタル署名

付加手段により、認証局側受信手段で受信されたデータを用いて、請求項９記載の情報認証装置と同一の方式により検査情報が生成され、生成された検査情報と認証局側受信手段で受信されたデータの認証情報として付加された検査情報とが所定関係を満たしているときは、認証局側受信手段で受信されたデータにディジタル署名が付加される。

【００６８】ここで、所定関係を満たすことには、例えば、照合対象の検査情報と被照合対象の検査情報とが一致していること、照合対象の検査情報を用いて所定演算式により演算を行った結果が被照合対象の検査情報と一致していること、または照合対象の検査情報を用いて所定演算式により演算を行った結果と被照合対象の検査情報を用いて所定演算式により演算を行った結果が一致すること、が挙げられる。

【００６９】さらに、本発明に係る請求項１９記載の認証局は、請求項１８記載の認証局において、前記ディジタル署名付加手段は、前記認証局側受信手段で受信したデータを用いて、請求項１０記載の情報認証装置と同一のハッシュ関数により検査情報を生成するようになっている。

【００７０】このような構成であれば、ディジタル署名付加手段により、認証局側受信手段で受信されたデータを用いて、請求項１０記載の情報認証装置と同一のハッシュ関数により検査情報が生成される。

【００７１】さらに、本発明に係る請求項２０記載の認証局は、請求項１４ないし１９のいずれかに記載の認証局において、前記ディジタル署名付加手段は、請求項１１記載の情報認証装置の暗号化方式と対応する復号化方式により前記認証局側受信手段で受信したデータを復号化するようになっている。

【００７２】このような構成であれば、ディジタル署名付加手段により、請求項１１記載の情報認証装置の暗号化方式と対応する復号化方式により認証局側受信手段で受信されたデータが復号化される。

【００７３】ここで、復号化方式は、どのようなものであってもよく、例えば、共通鍵復号化方式であってもよいし、公開鍵復号化方式であってもよい。これらの復号化方式としては、例えば、上記請求項１１の項目で例示した暗号化方式に対応したものが挙げられる。

【００７４】さらに、本発明に係る請求項２１記載の認証局は、請求項２０記載の認証局において、前記復号化方式は、公開鍵復号化方式であり、前記ディジタル署名付加手段は、前記認証局側受信手段で受信したデータを、当該データの送信元である情報認証装置の公開鍵で復号化するようになってる。

【００７５】このような構成であれば、ディジタル署名付加手段により、認証局側受信手段で受信されたデータが、そのデータの送信元である情報認証装置の公開鍵で復号化される。

【００７６】さらに、本発明に係る請求項２２記載の認証局は、請求項１４ないし２１のいずれかに記載の認証局において、前記ディジタル署名付加手段でディジタル署名を付加したデータを前記情報認証装置に送信する認証局側送信手段を備える。

【００７７】このような構成であれば、認証局側送信手段により、ディジタル署名付加手段でディジタル署名が付加されたデータが情報認証装置に送信される。

【００７８】さらに、本発明に係る請求項２３記載の認証局は、請求項１４ないし２１のいずれかに記載の認証局において、前記ディジタル署名付加手段でディジタル署名を付加したデータを記憶する認証局側データ記憶手段を備える。

【００７９】このような構成であれば、ディジタル署名付加手段でディジタル署名が付加されたデータが認証局側データ記憶手段に記憶される。

【００８０】以上では、上記目的を達成するための情報認証装置および認証局を提案したが、これに限らず、上記目的を達成するため、次の情報認証システムを提案することもできる。

【００８１】この情報認証システムは、ディジタル署名を行う認証局と情報認証装置とをネットワークを介して通信可能に接続したシステムであって、前記情報認証装置は、データを入力するデータ入力手段と、個人情報を入力する個人情報入力手段と、個人情報を記憶するための個人情報記憶手段と、当該情報認証装置に固有の情報である装置情報を記憶するための装置情報記憶手段と、前記データ入力手段でデータを入力したことを認証するための認証情報を前記データ入力手段で入力したデータに付加する認証情報付加手段と、前記認証情報付加手段で認証情報を付加したデータを前記認証局に送信する送信手段と、を備え、前記認証情報付加手段は、時間を測定する時間測定手段と、位置を測定する位置測定手段と、周囲の環境状態を測定する環境状態測定手段と、前記時間測定手段で測定した時間に基づいて前記データ入力手段でデータを入力した時点を特定するための時間情報を生成する時間情報生成手段と、前記位置測定手段で測定した位置に基づいて前記データ入力手段でデータを入力した地点を特定するための位置情報を生成する位置情報生成手段と、前記環境状態測定手段で測定した環境状態に基づいて前記データ入力手段でデータを入力した時点における環境状態を特定するための環境状態情報を生成する環境状態情報生成手段と、前記データ入力手段で入力したデータを用いて当該データに誤りが含まれているか否かを検査するための検査情報を生成する検査情報生成手段と、を有し、前記個人情報入力手段で入力した個人情報と前記個人情報記憶手段の個人情報とが所定関係を満たしているときは、生成した時間情報、位置情報、環境状態情報および検査情報を、並びに前記装置情報記憶手段の装置情報および前記個人情報記憶手段の個

人情報を認証情報として付加するようになっており、前記認証局は、前記情報認証装置からデータを受信する認証局側受信手段と、前記情報認証装置に固有の情報である装置情報を記憶するための認証局側装置情報記憶手段と、前記認証局側受信手段で受信したデータにディジタル署名を付加するディジタル署名付加手段と、を備え、前記ディジタル署名付加手段は、時間を測定する認証局側時間測定手段と、前記情報認証装置の位置を測定する認証局側位置測定手段と、前記認証局側受信手段で受信したデータを用いて前記検査情報生成手段と同一の方式により検査情報を生成する認証局側検査情報生成手段と、を有し、前記認証局側受信手段で受信したデータの認証情報として付加された時間情報により特定される時間と前記認証局側時間測定手段で測定した時間とが所定関係を満たしているとき、前記認証局側受信手段で受信したデータの認証情報として付加された位置情報により特定される位置と前記認証局側位置測定手段で測定した位置とが所定関係を満たしているとき、前記認証局側受信手段で受信したデータの認証情報として付加された装置情報と前記認証局側装置情報記憶手段の装置情報とが所定関係を満たしているとき、および、生成した検査情報と前記認証局側受信手段で受信したデータの認証情報として付加された検査情報とが所定関係を満たしているときは、前記認証局側受信手段で受信したデータにディジタル署名を付加するようになっている。

【００８２】このような構成であれば、情報認証装置では、データ入力手段でデータが入力されるとともに、個人情報入力手段で個人情報が入力されると、認証情報付加手段により、データ入力手段で入力されたデータに認証情報が付加され、送信手段により、認証情報付加手段で認証情報が付加されたデータが認証局に送信される。

【００８３】認証情報が付加される過程では、時間情報生成手段により、時間測定手段で測定された時間に基づいて時間情報が生成され、位置情報生成手段により、位置測定手段で測定された位置に基づいて位置情報が生成され、環境情報生成手段により、環境状態測定手段で測定された環境状態に基づいて環境状態情報が生成され、検査情報生成手段により、データ入力手段で入力されたデータを用いて検査情報が生成される。そして、入力された個人情報と個人情報記憶手段の個人情報とが所定関係を満たしているときは、生成された時間情報、位置情報、環境状態情報および検査情報が、並びに装置情報記憶手段の装置情報および個人情報記憶手段の個人情報が認証情報として付加される。

【００８４】一方、認証局では、認証局側受信手段により情報認証装置からデータが受信されると、ディジタル署名付加手段により、認証局側受信手段で受信されたデータに付加された認証情報に基づいて、データ入力手段でデータを入力したことが認証されたときは、認証局側受信手段で受信されたデータにディジタル署名が付加される。

【００８５】ディジタル署名が付加される過程では、認証局側検査情報生成手段により、認証局側受信手段で受信されたデータを用いて検査情報生成手段と同一の方式により検査情報が生成される。そして、認証局側受信手段で受信されたデータの認証情報として付加された時間情報により特定される時間と認証局側時間測定手段で測定された時間とが所定関係を満たしているとき、認証局側受信手段で受信されたデータの認証情報として付加された位置情報により特定される位置と認証局側位置測定手段で測定された位置とが所定関係を満たしているとき、認証局側受信手段で受信されたデータの認証情報として付加された装置情報と認証局側装置情報記憶手段の装置情報とが所定関係を満たしているとき、および、生成された検査情報と認証局側受信手段で受信されたデータの認証情報として付加された検査情報とが所定関係を満たしているときは、認証局側受信手段で受信されたデータにディジタル署名が付加される。

【００８６】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照しながら説明する。図１ないし図５は、本発明に係る情報認証装置および認証局の形態を示す図である。

【００８７】この実施の形態は、本発明に係る情報認証装置および認証局を、図１に示すように、ディジタルカメラ１０で取り込んだディジタル画像であるディジタルデータの認証を行う場合について適用したものである。

【００８８】まず、本発明に係る情報認証装置および認証局を適用する情報認証システムの構成を図１を参照しながら説明する。図１は、情報認証システムの構成を示すブロック図である。

【００８９】この情報認証システムは、図１に示すように、ディジタル署名を行う認証局２００と情報認証装置１００とをネットワークを介して通信可能に接続して構成されている。情報認証装置１００は、例えば、通常時は認証局２００と接続しておらず、ディジタルデータの認証を行うときにのみ認証局２００と接続するようになっている。なお、発明の理解を容易にするため、情報認証装置１００を１台しか図示していないが、実際には、異なる複数の情報認証装置が認証局２００に接続可能となっている。

【００９０】情報認証装置１００は、ディジタル画像であるディジタルデータを取り込むディジタルカメラ１０と、個人情報を入力する個人情報入力装置１２と、個人情報を記憶した個人情報記憶装置１４と、情報認証装置１００に固有の情報である装置情報を記憶した装置情報記憶装置１６と、ディジタルカメラ１０でディジタルデータを取り込んだことを認証するための認証情報をディジタルカメラ１０で取り込んだディジタルデータに付加する認証情報付加部１２０と、認証局２００とネットワークを介して通信する通信装置１８と、認証局２００で

ディジタル署名が付加されたディジタルデータを記憶するデータ記憶装置２０と、データ記憶装置２０のディジタルデータを外部に出力するための出力端子２２と、で構成されている。

【００９１】個人情報入力装置１２は、キーボード等の入力デバイスからなり、情報認証装置１００を利用する各利用者ごとに割り当てられたＩＤと、そのＩＤに対応したパスワードと、を入力するようになっている。

【００９２】個人情報記憶装置１４には、情報認証装置１００を利用する各利用者ごとに割り当てられたＩＤと、そのＩＤに対応したパスワードと、を暗号化した暗号化個人情報が格納されている。ここで、ＩＤおよびパスワードは、例えば、認証局２００において、個人ＩＤ用の暗号化アルゴリズムにより暗号化されたものである。

【００９３】装置情報記憶装置１６には、情報認証装置１００に固有の情報である装置情報（例えば、装置固有の番号）を暗号化した暗号化装置情報が格納されている。ここで、装置情報は、例えば、認証局２００において、装置用の暗号化アルゴリズムにより暗号化されたものである。

【００９４】通信装置１８は、携帯電話やＰＨＳ等を利用して、現在地点から最も近くにある基地局を特定し、無線により一般公衆回線網を通じてネットワークに接続し、そのネットワークを介してディジタルデータを認証局２００に送信するようになっている。

【００９５】次に、認証情報付加部１２０の構成を詳細に説明する。

【００９６】認証情報付加部１２０は、時間を測定する時間測定装置４２と、位置を測定する位置測定装置４４と、周囲の環境状態を測定する複数のセンサS_1～S_nと、個人情報入力装置１２で入力した個人情報と個人情報記憶装置１４の個人情報とを照合して利用者の認証を行う利用者認証装置４６と、認証情報を生成してこれをディジタルカメラ１０で取り込んだディジタルデータに付加する処理を行う情報処理装置４０と、で構成されている。

【００９７】時間測定装置４２は、現在の時刻を示す時刻信号を送信する周回衛星から時刻信号を受信し、受信した時刻信号に基づいて、現在の時刻を測定するようになっている。

【００９８】位置測定装置４４は、現在の時刻を示す時刻信号を送信する周回衛星から時刻信号を受信し、それら時刻信号により示される時刻のずれおよび各周回衛星の周回軌道に基づいて、位置を測定するいわゆるＧＰＳを利用して、現在地点の位置を測定するようになっている。

【００９９】センサS_1～S_nは、周囲の環境状態として、例えば、周囲の温度、湿度、気圧、ガス濃度、風速、標高、音量または光量を測定するようになっている。これらの物理量を測定するセンサとしては、既知の計測器を用いることができる。

【０１００】利用者認証装置４６は、情報処理装置４０から利用者の認証要求があったときは、個人情報入力装置１２でＩＤおよびパスワードを入力するとともに、個人情報記憶装置１４から暗号化個人情報を読み出してこれを復号化し、入力したＩＤおよびパスワードと、復号化したＩＤおよびパスワードと、が一致するか否かを判定するようになっている。判定の結果、これらが一致すると判定されたときは、正当な利用者であることを示す利用者認証データを情報処理装置４０に出力し、これらが一致しないと判定されたときは、不正な利用者であることを示す利用者認証データを情報処理装置４０に出力するようになっている。

【０１０１】次に、情報処理装置４０の構成を図２を参照しながら説明する。図２は、情報処理装置４０の構成を示すブロック図である。

【０１０２】情報処理装置４０は、図２に示すように、制御プログラムに基づいて演算およびシステム全体を制御するＣＰＵ６０と、所定領域にあらかじめＣＰＵ６０の制御プログラム等を格納しているＲＯＭ６２と、ＲＯＭ６２等から読み出したデータやＣＰＵ６０の演算過程で必要な演算結果を格納するためのＲＡＭ６４と、外部装置に対してデータの入出力を媒介するＩ／Ｆ６８と、で構成されており、これらは、データを転送するための信号線であるバス６９で相互にかつデータ授受可能に接続されている。

【０１０３】Ｉ／Ｆ６８には、外部装置として、ディジタルカメラ１０と、個人情報記憶装置１４と、装置情報記憶装置１６と、通信装置１８と、データ記憶装置２０と、出力端子２２と、時間測定装置４２と、位置測定装置４４と、センサS_1～S_nと、利用者認証装置４６と、が接続されている。

【０１０４】ＣＰＵ６０は、マイクロプロセッシングユニットＭＰＵ等からなり、電源が投入されたときは、ＲＯＭ６２の所定領域に格納されている所定のプログラムを起動させ、そのプログラムに従って、図３のフローチャートに示す認証情報付加処理を実行するようになっている。図３は、認証情報付加処理を示すフローチャートである。

【０１０５】認証情報付加処理は、Ｉ／Ｆ６８に接続された外部装置を利用して認証情報を生成し、生成した認証情報をディジタルカメラ１０で取り込んだディジタルデータに付加する処理であって、ＣＰＵ６０において実行されると、図３に示すように、まず、ステップＳ１００に移行するようになっている。

【０１０６】ステップＳ１００では、利用者の認証要求を利用者認証装置４６に出力し、ステップＳ１０２に移行して、利用者認証データを利用者認証装置４６から入力し、入力した利用者認証データが正当な利用者である

ことを示しているか否かを判定し、正当な利用者であることを示していると判定されたとき(Yes)は、ステップＳ１０４に移行する。

【０１０７】ステップＳ１０４では、ディジタル画像であるディジタルデータをディジタルカメラ１０から入力したか否かを判定し、ディジタルデータを入力したと判定したとき(Yes)は、ステップＳ１０６に移行して、時間測定装置４２から現在の時刻を入力し、入力した時刻に基づいて、ディジタルカメラ１０でディジタルデータを入力した時点を特定するための時間情報を生成し、ステップＳ１０８に移行する。

【０１０８】ステップＳ１０８では、位置測定装置４４から現在地点の位置を入力し、入力した位置に基づいて、ディジタルカメラ１０でディジタルデータを入力した地点を特定するための位置情報を生成し、ステップＳ１１０に移行して、センサS_1～S_nから周囲の環境状態を入力し、入力した環境状態に基づいて、ディジタルカメラ１０でディジタルデータを入力した時点における環境状態を特定するための環境状態情報を生成し、ステップＳ１１２に移行する。

【０１０９】ステップＳ１１２では、個人情報記憶装置１４から個人情報を読み出し、ステップＳ１１４に移行して、装置情報記憶装置１６から装置情報を読み出し、ステップＳ１１６に移行して、生成した時間情報、位置情報および環境状態情報を、並びに読み出した個人情報および装置情報を認証情報としてディジタルカメラ１０で入力したディジタルデータに付加し、ステップＳ１１８に移行する。具体的にステップＳ１１６では、例えば、認証情報を電子透かしやサブリミナル情報としてディジタルデータに付加する。

【０１１０】ステップＳ１１８では、認証情報を付加したディジタルデータを所定のハッシュ関数に代入することにより、そのディジタルデータに誤りが含まれているか否かを検査するための検査情報を、そのハッシュ関数により得られるハッシュ値として生成し、ステップＳ１２０に移行して、生成した検査情報を認証情報としてディジタルカメラ１０で入力したディジタルデータにさらに付加し、ステップＳ１２２に移行する。具体的にステップＳ１２２では、例えば、認証情報を電子透かしやサブリミナル情報としてディジタルデータに付加する。

【０１１１】ステップＳ１２２では、公開鍵暗号化方式により、認証情報を付加したディジタルデータを情報認証装置１００の秘密鍵で暗号化し、ステップＳ１２４に移行して、暗号化したディジタルデータを通信装置１８に出力して認証局２００に送信し、ステップＳ１２６に移行する。

【０１１２】ステップＳ１２６では、認証局２００でディジタル署名が付加されたディジタルデータを認証局２００から受信して通信装置１８から入力したか否かを判定し、ディジタル署名が付加されたディジタルデータを入力したと判定されたとき(Yes)は、ステップＳ１２８に移行して、入力したディジタルデータをデータ記憶装置２０に格納し、ステップＳ１３０に移行する。

【０１１３】ステップＳ１３０では、ディジタルデータの出力要求が利用者からあるか否かを判定し、ディジタルデータの出力要求があると判定されたとき(Yes)は、ステップＳ１３２に移行して、データ記憶装置２０のディジタルデータを出力端子２２に出力し、ステップＳ１０４に移行する。

【０１１４】一方、ステップＳ１３０で、ディジタルデータの出力要求が利用者からないと判定されたとき(No)は、ステップＳ１０４に移行する。

【０１１５】一方、ステップＳ１２６で、ディジタル署名が付加されたディジタルデータを通信装置１８から入力しないと判定されたとき(No)は、ディジタルデータを入力するまでステップＳ１２６で待機する。

【０１１６】一方、ステップＳ１０４で、ディジタルカメラ１０からディジタルデータを入力しないと判定されたとき(No)は、ステップＳ１３０に移行する。

【０１１７】一方、ステップＳ１０２で、利用者認証データが不正な利用者であることを示していると判定されたとき(No)は、ステップＳ１３４に移行して、強制的に電源を遮断し、一連の処理を終了する。

【０１１８】次に、図１に戻り、認証局２００の構成を説明する。

【０１１９】認証局２００は、図１に示すように、情報認証装置１００とネットワークを介して通信する通信装置２４と、個人情報を記憶した個人情報記憶装置２６と、装置情報を記憶した装置情報記憶装置２８と、通信装置２４で受信したディジタルデータにディジタル署名を付加するディジタル署名付加部２２０と、で構成されている。

【０１２０】個人情報記憶装置２６には、個人情報記憶装置１４に格納されているものと同一のＩＤおよびパスワードであって、装置情報記憶装置２８の装置情報により特定される情報認証装置を利用する各利用者ごとに割り当てられたＩＤと、そのＩＤに対応したパスワードと、が格納されている。また、個人情報記憶装置２６の個人情報は、装置情報記憶装置２８の装置情報と関連づけられており、すなわち、その関連づけにより、装置情報記憶装置２８の装置情報により特定される情報認証装置について、その利用者のＩＤおよびパスワードを特定することが可能となる。なお、この関連づけは、情報認証装置１００を利用しようとする者が、利用する前に認証局２００に届け出ることにより行われる。

【０１２１】次に、ディジタル署名付加部２２０の構成を詳細に説明する。

【０１２２】ディジタル署名付加部２２０は、時間を測定する時間測定装置５２と、情報認証装置１００の位置を測定する位置測定装置５４と、通信装置２４で受信し

たディジタルデータにディジタル署名を付加する処理を行う情報処理装置５０と、で構成されている。

【０１２３】時間測定装置５２は、時間測定装置４２と同一機能を有して構成されており、現在の時刻を示す時刻信号を送信する周回衛星から時刻信号を受信し、受信した時刻信号に基づいて、現在の時刻を測定するようになっている。

【０１２４】位置測定装置５４は、通信装置２４が情報認証装置１００と通信を行っている間に、情報認証装置１００が通信している基地局を特定することにより、情報認証装置１００の位置を測定するようになっている。なお、基地局の特定方法は、従来の方法による。

【０１２５】次に、情報処理装置５０の構成を図４を参照しながら説明する。図４は、情報処理装置５０の構成を示すブロック図である。

【０１２６】情報処理装置５０は、図４に示すように、制御プログラムに基づいて演算およびシステム全体を制御するＣＰＵ７０と、所定領域にあらかじめＣＰＵ７０の制御プログラム等を格納しているＲＯＭ７２と、ＲＯＭ７２等から読み出したデータやＣＰＵ７０の演算過程で必要な演算結果を格納するためのＲＡＭ７４と、外部装置に対してデータの入出力を媒介するＩ／Ｆ７８と、で構成されており、これらは、データを転送するための信号線であるバス７９で相互にかつデータ授受可能に接続されている。

【０１２７】Ｉ／Ｆ７８には、外部装置として、通信装置２４と、個人情報記憶装置２６と、装置情報記憶装置２８と、時間測定装置５２と、位置測定装置５４と、が接続されている。

【０１２８】ＣＰＵ７０は、マイクロプロセッシングユニットＭＰＵ等からなり、ＲＯＭ７２の所定領域に格納されている所定のプログラムを起動させ、そのプログラムに従って、常時、図５のフローチャートに示すディジタル署名付加処理を実行するようになっている。図５は、ディジタル署名付加処理を示すフローチャートである。

【０１２９】ディジタル署名付加処理は、通信装置２４で受信したディジタルデータにディジタル署名を付加する処理であって、ＣＰＵ７０において実行されると、図５に示すように、まず、ステップＳ２００に移行するようになっている。

【０１３０】ステップＳ２００では、ディジタルデータを情報認証装置１００から受信して通信装置２４から入力したか否かを判定し、ディジタルデータを入力したと判定されたとき(Yes)は、ステップＳ２０２に移行して、公開鍵復号化方式により、入力したディジタルデータを、そのディジタルデータの送信元である情報認証装置１００の公開鍵で復号化し、ステップＳ２０４に移行する。

【０１３１】ステップＳ２０４では、時間測定装置５２から現在の時刻を入力し、復号化したディジタルデータの認証情報として付加された時間情報により特定される時刻と時間測定装置５２から入力した時刻との時間差が所定範囲内（例えば、１分）であるか否かを判定し、その時間差が所定範囲内であると判定されたとき(Yes)は、ステップＳ２０６に移行する。

【０１３２】ステップＳ２０６では、ディジタルデータの送信元である情報認証装置１００の位置を位置測定装置５４から入力し、復号化したディジタルデータの認証情報として付加された位置情報により特定される位置が、位置測定装置５４から入力した位置を中心として所定範囲（例えば、半径３００ｍ）の領域内に含まれているか否かを判定し、所定範囲の領域内に含まれていると判定されたとき(Yes)は、ステップＳ２０８に移行する。

【０１３３】ステップＳ２０８では、復号化したディジタルデータの認証情報として付加された装置情報を復号化し、ステップＳ２１０に移行して、復号化した装置情報をもとに装置情報記憶装置２８を検索し、ステップＳ２１２に移行して、復号化した装置情報に該当する装置情報を索出したか否かを判定し、該当する装置情報を索出したと判定されたとき(Yes)は、ステップＳ２１４に移行する。

【０１３４】ステップＳ２１４では、復号化したディジタルデータの認証情報として付加された個人情報を復号化し、ステップＳ２１６に移行して、ステップＳ２１２で索出した装置情報をもとに、個人情報記憶装置２６を検索して関連する個人情報を読み出し、ステップＳ２１８に移行して、復号化した個人情報であるＩＤおよびパスワードと、読み出した個人情報であるＩＤおよびパスワードと、が一致しているか否かを判定し、これらが一致していると判定されたとき(Yes)は、ステップＳ２２０に移行する。

【０１３５】ステップＳ２２０では、復号化したディジタルデータのうち認証情報として付加された検査情報を除いた部分を、上記ステップＳ１１８と同一のハッシュ関数に代入することにより、そのディジタルデータに誤りが含まれているか否かを検査するための検査情報を、そのハッシュ関数により得られるハッシュ値として生成し、ステップＳ２２２に移行して、生成した検査情報と、復号化したディジタルデータの認証情報として付加された検査情報と、が一致しているか否かを判定し、これらが一致していると判定されたとき(Yes)は、ステップＳ２２４に移行する。

【０１３６】ステップＳ２２４では、復号化したディジタルデータにディジタル署名を付加し、ステップＳ２２６に移行して、公開鍵暗号化方式により、ディジタル署名を付加したディジタルデータを認証局２００の秘密鍵で暗号化し、ステップＳ２２８に移行して、暗号化したディジタルデータを通信装置２４に出力して、そのディ

ジタルデータの送信元である情報認証装置１００に送信し、ステップＳ２００に移行する。

【０１３７】一方、ステップＳ２２２では、ハッシュ関数により生成した検査情報と、復号化したディジタルデータの認証情報として付加された検査情報と、が一致していないと判定されたとき(No)は、不正なディジタルデータであるとしてディジタル署名を付加せず、ステップＳ２００に移行する。

【０１３８】一方、ステップＳ２１８では、復号化した個人情報であるＩＤおよびパスワードと、読み出した個人情報であるＩＤおよびパスワードと、が一致していないと判定されたとき(No)は、不正なディジタルデータであるとしてディジタル署名を付加せず、ステップＳ２００に移行する。

【０１３９】一方、ステップＳ２１２では、復号化した装置情報に該当する装置情報を装置情報記憶装置２８から索出しないと判定されたとき(No)は、不正なディジタルデータであるとしてディジタル署名を付加せず、ステップＳ２００に移行する。

【０１４０】一方、ステップＳ２０６では、復号化したディジタルデータの認証情報として付加された位置情報により特定される位置が、位置測定装置５４から入力した位置を中心として所定範囲の領域内に含まれていないと判定されたとき(No)は、不正なディジタルデータであるとしてディジタル署名を付加せず、ステップＳ２００に移行する。

【０１４１】一方、ステップＳ２０４では、復号化したディジタルデータの認証情報として付加された時間情報により特定される時刻と時間測定装置５２から入力した時刻との時間差が所定範囲外であると判定されたとき(No)は、不正なディジタルデータであるとしてディジタル署名を付加せず、ステップＳ２００に移行する。

【０１４２】一方、ステップＳ２００では、ディジタルデータを通信装置２４から入力しないと判定されたとき(No)は、ディジタルデータを入力するまでステップＳ２００で待機する。

【０１４３】次に、上記実施の形態の動作を説明する。

【０１４４】利用者は、ディジタルカメラ１０でディジタル画像を取り込むには、まず、情報認証装置１００に電源を投入し、ＩＤおよびパスワードを個人情報入力装置１２から入力する。

【０１４５】ここで、利用者が認証局２００に届け出た正当なＩＤおよびパスワードを入力したものとすると、情報認証装置１００では、利用者認証装置４６により、個人情報記憶装置１４から暗号化個人情報が読み出されてこれが復号化され、個人情報入力装置１２から入力されたＩＤおよびパスワードと、復号化されたＩＤおよびパスワードと、が一致するので、正当な利用者であることを示す利用者認証データが情報処理装置４０に出力される。情報処理装置４０では、正当な利用者であることを示す利用者認証データが入力されると、ＣＰＵ６０により、ステップＳ１００，Ｓ１０２を経て、正当な利用者であると認証され、ディジタルカメラ１０でディジタル画像を取り込み可能な状態となる。

【０１４６】この状態で、利用者がディジタルカメラ１０でディジタル画像を取り込むと、情報処理装置４０では、ディジタルカメラ１０からディジタルデータが入力されるので、ステップＳ１０６～Ｓ１１６を経て、時間測定装置４２で測定された時刻に基づいて時間情報が生成され、位置測定装置４４で測定された位置に基づいて位置情報が生成され、センサS_1～S_nで測定された環境状態に基づいて環境状態情報が生成される。次いで、個人情報記憶装置１４から個人情報が読み出され、装置情報記憶装置１６から装置情報が読み出され、生成された時間情報、位置情報および環境状態情報が、並びに読み出された個人情報および装置情報が認証情報としてディジタルカメラ１０で入力されたディジタルデータに付加される。

【０１４７】次いで、ステップＳ１１８～Ｓ１２４を経て、認証情報が付加されたディジタルデータを用いてハッシュ関数により検査情報がハッシュ値として生成され、生成された検査情報が認証情報としてディジタルカメラ１０で入力されたディジタルデータにさらに付加され、認証情報が付加されたディジタルデータが情報認証装置１００の秘密鍵で暗号化され、暗号化されたディジタルデータが通信装置１８に出力される。そして、通信装置１８により、現在地点から最も近くにある基地局が特定され、無線により一般公衆回線網を通じてネットワークに接続され、そのネットワークを介してディジタルデータが認証局２００に送信される。

【０１４８】一方、認証局２００では、通信装置２４により、情報認証装置１００からディジタルデータが受信されると、受信されたディジタルデータが情報処理装置５０に出力される。情報処理装置５０では、ディジタルデータが通信装置２４から入力されると、ＣＰＵ７０により、ステップＳ２０２，Ｓ２０４を経て、入力されたディジタルデータが情報認証装置１００の公開鍵で復号化され、復号化されたディジタルデータの認証情報として付加された時間情報により特定される時刻と時間測定装置５２で測定された時刻との時間差が所定範囲内であるか否かが判定されるが、認証情報として付加された時間情報は、情報認証装置１００で生成された正当なものであるので、ここでは、その時間差が所定範囲内であると判定される。

【０１４９】次いで、ステップＳ２０６を経て、復号化されたディジタルデータの認証情報として付加された位置情報により特定される位置が、位置測定装置５４で測定された位置を中心として所定範囲の領域内に含まれているか否かが判定されるが、認証情報として付加された位置情報は、情報認証装置１００で生成された正当なも

のであるので、ここでは、位置情報により特定される位置が所定範囲の領域内に含まれると判定される。

【０１５０】次いで、ステップＳ２０８～Ｓ２１２を経て、復号化されたディジタルデータの認証情報として付加された装置情報が復号化され、復号化された装置情報をもとに装置情報記憶装置２８が検索され、復号化された装置情報に該当する装置情報が索出されたか否かが判定されるが、復号化された装置情報は、情報認証装置１００で与えられた正当なものであることから、同一の装置情報が装置情報記憶装置２８に登録されているので、ここでは、該当する装置情報が索出されたと判定される。

【０１５１】次いで、ステップＳ２１４～Ｓ２１８を経て、復号化されたディジタルデータの認証情報として付加された個人情報が復号化され、索出された装置情報をもとに、個人情報記憶装置２６が検索されて関連する個人情報が読み出され、復号化された個人情報であるＩＤおよびパスワードと、読み出された個人情報であるＩＤおよびパスワードと、が一致しているか否かが判定されるが、復号化された個人情報は、情報認証装置１００で与えられた正当なものであるので、ここでは、これらが一致していると判定される。

【０１５２】次いで、ステップＳ２２０，Ｓ２２２を経て、復号化されたディジタルデータのうち認証情報として付加された検査情報を除いた部分を用いて、ハッシュ関数により検査情報がハッシュ値として生成され、生成された検査情報と、復号化されたディジタルデータの認証情報として付加された検査情報と、が一致しているか否かが判定されるが、認証情報として付加された検査情報は、情報認証装置１００で生成された正当なものであるので、ここでは、これらが一致していると判定される。

【０１５３】次いで、ステップＳ２２４～Ｓ２２８を経て、復号化されたディジタルデータにディジタル署名が付加され、ディジタル署名が付加されたディジタルデータが認証局２００の秘密鍵で暗号化され、暗号化されたディジタルデータが通信装置２４に出力される。そして、通信装置２４により、ネットワークを介してディジタルデータが情報認証装置１００に送信される。

【０１５４】一方、情報認証装置１００では、通信装置１８により、認証局２００からディジタルデータが受信されると、受信されたディジタルデータが情報処理装置４０に出力される。情報処理装置４０では、ディジタルデータが通信装置１８から入力されると、ＣＰＵ６０により、ステップＳ１２６，Ｓ１２８を経て、入力されたディジタルデータがデータ記憶装置２０に格納される。

【０１５５】ここで、利用者がディジタルデータの出力要求を行うと、ステップＳ１３０，Ｓ１３２を経て、データ記憶装置２０のディジタルデータが出力端子２２に出力される。出力端子２２から出力されたディジタルデータは、例えば、フロッピー（登録商標）ディスク等に記憶される。

【０１５６】なお、不正行為等により、認証情報が付加されたディジタルデータのうち、ディジタルデータ、時間情報、位置情報、個人情報、装置情報および検査情報のいずれかが改ざんされた場合は、認証局２００において、ステップＳ２０４、Ｓ２０６、Ｓ２１２、Ｓ２１８およびＳ２２２のいずれかのステップを経て、不正なディジタルデータであると判定され、ディジタル署名が付加されない。

【０１５７】また、不正行為等により、認証局２００で受信したディジタルデータが、そのディジタルデータの送信元である情報認証装置１００の秘密鍵以外の鍵で暗号化されている場合には、認証局２００において、ステップＳ２０２を経て、ディジタルデータが復号化されないので、不正なディジタルデータであるとして処理される。

【０１５８】また、不正行為等により、認証局２００以外でディジタル署名が付加された場合には、情報認証装置１００から出力されたディジタルデータが、認証局２００の公開鍵で復号化することができないので、不正なディジタルデータであることが分かる。

【０１５９】また、情報認証装置１００への電源投入時に、利用者が認証局２００に届け出ていない不正なＩＤおよびパスワードを入力した場合には、情報認証装置１００において、ステップＳ１０２，Ｓ１３４を経て、強制的に電源が遮断される。

【０１６０】このようにして、本実施の形態では、情報認証装置１００は、ディジタルデータを取り込むディジタルカメラ１０と、外部から取得した情報に基づいて認証情報を生成してこれをディジタルカメラ１０で入力したディジタルデータに付加する認証情報付加部１２０と、を備えた。

【０１６１】これにより、内部で生成した情報に基づいて生成した認証情報を付加する場合に比して、ディジタルデータに付加された認証情報が客観性を有するので、従来に比して、ディジタルデータの客観性を確保することができ、ディジタルデータの証拠としての証明力を向上することができる。

【０１６２】さらに、本実施の形態では、ディジタルデータを取り込むディジタルカメラ１０と、ディジタルカメラ１０で入力したディジタルデータに認証情報を付加する認証情報付加部１２０と、認証情報付加部１２０で認証情報を付加したディジタルデータを認証局２００に送信する通信装置１８と、を備えた。

【０１６３】これにより、内部で生成した情報に基づいて生成した認証情報を付加する場合に比して、ディジタルデータに付加された認証情報が客観性を有するので、従来に比して、ディジタルデータの客観性を確保することができ、ディジタルデータの証拠としての証明力を向

上することができる。

【０１６４】さらに、本実施の形態では、認証情報付加部１２０は、時間測定装置４２で測定した時間に基づいて時間情報を生成し、生成した時間情報を認証情報として付加するようにした。

【０１６５】これにより、ディジタルデータに付加された認証情報から、ディジタルデータを入力した時点を特定することができ、しかもその認証情報が客観性を有するので、ディジタルデータの証拠としての証明力をさらに向上することができる。

【０１６６】さらに、本実施の形態では、認証情報付加部１２０は、位置測定装置４４で測定した位置に基づいて位置情報を生成し、生成した位置情報を認証情報として付加するようにした。

【０１６７】これにより、ディジタルデータに付加された認証情報から、ディジタルデータを入力した地点を特定することができ、しかもその認証情報が客観性を有するので、ディジタルデータの証拠としての証明力をさらに向上することができる。

【０１６８】さらに、本実施の形態では、認証情報付加部１２０は、センサS_1～S_nで測定した環境状態に基づいて環境状態情報を生成し、生成した環境状態情報を認証情報として付加するようにした。

【０１６９】これにより、ディジタルデータに付加された認証情報から、ディジタルデータを入力した時点における環境状態を特定することができ、しかもその認証情報が客観性を有するので、ディジタルデータの証拠としての証明力をさらに向上することができる。

【０１７０】さらに、本実施の形態では、認証情報付加部１２０は、個人情報入力装置１２で入力した個人情報と個人情報記憶装置１４の個人情報とが一致しているときは、個人情報記憶装置１４の個人情報を認証情報として付加するようにした。

【０１７１】これにより、ディジタルデータに付加された認証情報から、ディジタルデータを入力した利用者を特定することができ、しかもその認証情報が客観性を有するので、ディジタルデータの証拠としての証明力をさらに向上することができる。

【０１７２】さらに、本実施の形態では、認証情報付加部１２０は、装置情報記憶装置１６の装置情報を認証情報として付加するようにした。

【０１７３】これにより、ディジタルデータに付加された認証情報から、ディジタルデータを入力した装置を特定することができ、しかもその認証情報が客観性を有するので、ディジタルデータの証拠としての証明力をさらに向上することができる。

【０１７４】さらに、本実施の形態では、認証情報付加部１２０は、ディジタルカメラ１０で入力したディジタルデータを用いて検査情報を生成し、生成した検査情報を認証情報として付加するようにした。

【０１７５】これにより、ディジタルデータに付加された認証情報から、ディジタルデータが改ざんされているか否かが分かり、しかもその認証情報が客観性を有するので、ディジタルデータの証拠としての証明力をさらに向上することができる。

【０１７６】さらに、本実施の形態では、認証情報付加部１２０は、公開鍵暗号化方式により、認証情報を付加したディジタルデータを情報認証装置１００の秘密鍵で暗号化するようにした。

【０１７７】これにより、認証局２００では、受信したディジタルデータが、そのディジタルデータの送信元である情報認証装置１００の公開鍵でしか復号化することができないので、復号化できたときは、情報認証装置１００で入力したディジタルデータが確かにその情報認証装置１００から送信されたものであるということが分かり、復号化できなかったときは、そうでないことが分かるので、ディジタルデータの証拠としての証明力をさらに向上することができる。

【０１７８】一方、本実施の形態では、認証局２００は、情報認証装置１００からディジタルデータを受信する通信装置２４と、通信装置２４で受信したディジタルデータにディジタル署名を付加するディジタル署名付加部２２０と、を備え、ディジタル署名付加部２２０は、通信装置２４で受信したディジタルデータに付加された認証情報に基づいて、ディジタルカメラ１０でディジタルデータを入力したことを認証したときは、通信装置２４で受信したディジタルデータにディジタル署名を付加するようにした。

【０１７９】これにより、ディジタルデータに付加された認証情報が改ざんされたりディジタルデータが不正な方法で送信されたりした場合には、ディジタルデータにディジタル署名が付加されないので、従来に比して、ディジタルデータの客観性を確保することができ、ディジタルデータの証拠としての証明力を向上することができる。

【０１８０】さらに、本実施の形態では、ディジタル署名付加部２２０は、通信装置２４で受信したディジタルデータの認証情報として付加された時間情報により特定される時間と時間測定装置５２で測定した時間との時間差が所定範囲内であるときは、通信装置２４で受信したディジタルデータにディジタル署名を付加するようにした。

【０１８１】これにより、ディジタルデータの認証情報として付加された時間情報が改ざんされた場合には、ディジタルデータにディジタル署名が付加されないので、ディジタルデータの客観性をさらに確保することができ、ディジタルデータの証拠としての証明力をより一層向上することができる。

【０１８２】さらに、本実施の形態では、ディジタル署名付加部２２０は、通信装置２４で受信したディジタル

データの認証情報として付加された位置情報により特定される位置が、位置測定装置５４で測定した位置を中心として所定範囲の領域内に含まれているときは、通信装置２４で受信したディジタルデータにディジタル署名を付加するようにした。

【０１８３】これにより、ディジタルデータの認証情報として付加された位置情報が改ざんされた場合には、ディジタルデータにディジタル署名が付加されないので、ディジタルデータの客観性をさらに確保することができ、ディジタルデータの証拠としての証明力をより一層向上することができる。

【０１８４】さらに、本実施の形態では、ディジタル署名付加部２２０は、通信装置２４で受信したディジタルデータの認証情報として付加された装置情報と装置情報記憶装置２８の装置情報とが一致しているときは、通信装置２４で受信したディジタルデータにディジタル署名を付加するようにした。

【０１８５】これにより、ディジタルデータの認証情報として付加された装置情報が改ざんされた場合には、ディジタルデータにディジタル署名が付加されないので、ディジタルデータの客観性をさらに確保することができ、ディジタルデータの証拠としての証明力をより一層向上することができる。

【０１８６】さらに、本実施の形態では、ディジタル署名付加部２２０は、通信装置２４で受信したディジタルデータを用いて検査情報を生成し、生成した検査情報と通信装置２４で受信したディジタルデータの認証情報として付加された検査情報とが一致しているときは、通信装置２４で受信したディジタルデータにディジタル署名を付加するようにした。

【０１８７】これにより、ディジタルデータの認証情報として付加された検査情報やディジタルデータ自体が改ざんされた場合には、ディジタルデータにディジタル署名が付加されないので、ディジタルデータの客観性をさらに確保することができ、ディジタルデータの証拠としての証明力をより一層向上することができる。

【０１８８】なお、上記実施の形態において、認証局２００は、ディジタル署名を付加したディジタルデータを情報認証装置１００に送信する際に、ディジタルデータに情報を付加するようには特に構成しなかったが、これに限らず、ステップＳ２２２を経た後、通信装置２４で受信したディジタルデータ（認証情報を含む。）を所定のハッシュ関数に代入することにより、そのディジタルデータに誤りが含まれているか否かを検査するための検査情報を、そのハッシュ関数により得られるハッシュ値として生成し、生成した検査情報をそのディジタルデータに付加するように構成してもよい。

【０１８９】このような構成であれば、情報認証装置１００において、付加された検査情報によりディジタルデータの正当性を検証することができるので、ディジタルデータの客観性をさらに確保することができ、ディジタルデータの証拠としての証明力をより一層向上することができる。

【０１９０】また、上記実施の形態において、認証局２００は、ディジタル署名を付加したディジタルデータを情報認証装置１００に送信し、情報認証装置１００は、受信したディジタルデータをデータ記憶装置２０に格納するように構成したが、これに限らず、認証局２００は、ディジタルデータを記憶するデータ記憶装置を備え、ディジタル署名を付加したディジタルデータをデータ記憶装置に格納するように構成してもよい。この場合、情報認証装置１００は、データ記憶装置２０および出力端子２２を設けずに構成することができる。

【０１９１】また、上記実施の形態において、情報認証装置１００は、時間測定装置４２を設け、認証情報として時間情報をディジタルデータに付加するように構成したが、これに限らず、時間測定装置４２を設けず、時間情報を付加しないように構成することもできる。この場合、認証局２００は、時間測定装置５２を設けず、時間情報による判定を行わないように構成することができる。

【０１９２】また、上記実施の形態において、情報認証装置１００は、位置測定装置４４を設け、認証情報として位置情報をディジタルデータに付加するように構成したが、これに限らず、位置測定装置４４を設けず、位置情報を付加しないように構成することもできる。この場合、認証局２００は、位置測定装置５４を設けず、位置情報による判定を行わないように構成することができる。

【０１９３】また、上記実施の形態において、情報認証装置１００は、センサS_1～S_nを設け、認証情報として環境状態情報をディジタルデータに付加するように構成したが、これに限らず、センサS_1～S_nを設けず、環境状態情報を付加しないように構成することもできる。

【０１９４】また、上記実施の形態において、情報認証装置１００は、個人情報入力装置１２、個人情報記憶装置１４および利用者認証装置４６を設け、認証情報として個人情報をディジタルデータに付加するように構成したが、これに限らず、これら装置を設けず、個人情報を付加しないように構成することもできる。この場合、認証局２００は、個人情報記憶装置２６を設けず、個人情報による判定を行わないように構成することができる。

【０１９５】また、上記実施の形態において、情報認証装置１００は、装置情報記憶装置１６を設け、認証情報として装置情報をディジタルデータに付加するように構成したが、これに限らず、装置情報記憶装置１６を設けず、装置情報を付加しないように構成することもできる。この場合、認証局２００は、装置情報記憶装置２８を設けず、装置情報による判定を行わないように構成することができる。

【０１９６】また、上記実施の形態において、情報認証装置１００は、認証情報として検査情報をディジタルデータに付加するように構成したが、これに限らず、検査情報を付加しないように構成することもできる。この場合、認証局２００は、検査情報による判定を行わないように構成することができる。

【０１９７】また、上記実施の形態において、情報認証装置１００は、認証情報を付加したディジタルデータを暗号化して送信するように構成したが、これに限らず、認証情報を付加したディジタルデータを暗号化せずに送信するように構成することもできる。この場合、認証局２００は、受信したディジタルデータを復号化しないように構成することができる。

【０１９８】また、上記実施の形態において、図３および図５のフローチャートに示す処理を実行するにあたってはいずれも、ＲＯＭ６２，７２にあらかじめ格納されている制御プログラムを実行する場合について説明したが、これに限らず、これらの手順を示したプログラムが記憶された記憶媒体から、そのプログラムをＲＡＭ６４，７４に読み込んで実行するようにしてもよい。

【０１９９】ここで、記憶媒体とは、ＲＡＭ、ＲＯＭ等の半導体記憶媒体、ＦＤ、ＨＤ等の磁気記憶型記憶媒体、ＣＤ、ＣＤＶ、ＬＤ、ＤＶＤ等の光学的読取方式記憶媒体、ＭＯ等の磁気記憶型／光学的読取方式記憶媒体であって、電子的、磁気的、光学的等の読み取り方法のいかんにかかわらず、コンピュータで読み取り可能な記憶媒体であれば、あらゆる記憶媒体を含むものである。

【０２００】上記実施の形態において、ディジタルカメラ１０は、請求項１ないし６、９または１０記載のデータ入力手段に対応し、認証情報付加部１２０は、請求項１ないし１２記載の認証情報付加手段に対応し、通信装置１８は、請求項３記載の送信手段および請求項１３記載の受信手段に対応し、時間測定装置４２は、請求項４記載の時間測定手段に対応し、位置測定装置４４は、請求項２または５記載の位置測定手段に対応している。

【０２０１】また、上記実施の形態において、センサS_1～S_nは、請求項６記載の環境状態測定手段に対応し、個人情報入力装置１２は、請求項７記載の個人情報入力手段に対応し、個人情報記憶装置１４は、請求項７記載の個人情報記憶手段に対応し、装置情報記憶装置１６は、請求項８記載の装置情報記憶手段に対応し、データ記憶装置２０は、請求項１３記載のデータ記憶手段に対応している。

【０２０２】また、上記実施の形態において、通信装置２４は、請求項１４ないし２１記載の受信手段および請求項２３記載の送信手段に対応し、ディジタル署名付加部２２０は、請求項１４ないし２３記載のディジタル署名付加手段に対応し、時間測定装置５２は、請求項１５記載の認証局側時間測定手段に対応し、位置測定装置５４は、請求項１６記載の認証局側位置測定手段に対応し、装置情報記憶装置２６は、請求項１７記載の認証局側装置情報記憶手段に対応している。

【０２０３】

【発明の効果】以上説明したように、本発明に係る請求項１ないし１３記載の情報認証装置によれば、データに付加された認証情報が客観性を有するので、従来に比して、データの客観性を確保することができ、データの証拠としての証明力を向上することができるという効果が得られる。

【０２０４】さらに、本発明に係る請求項４記載の情報認証装置によれば、データに付加された認証情報から、データを入力した時点を特定することができ、しかもその認証情報が客観性を有するので、データの証拠としての証明力をさらに向上することができるという効果も得られる。

【０２０５】さらに、本発明に係る請求項２または５記載の情報認証装置によれば、データに付加された認証情報から、データを入力した地点を特定することができ、しかもその認証情報が客観性を有するので、データの証拠としての証明力をさらに向上することができるという効果も得られる。

【０２０６】さらに、本発明に係る請求項６記載の情報認証装置によれば、データに付加された認証情報から、データを入力した時点における環境状態を特定することができ、しかもその認証情報が客観性を有するので、データの証拠としての証明力をさらに向上することができるという効果も得られる。

【０２０７】さらに、本発明に係る請求項７記載の情報認証装置によれば、データに付加された認証情報から、データを入力した利用者を特定することができ、しかもその認証情報が客観性を有するので、データの証拠としての証明力をさらに向上することができるという効果も得られる。

【０２０８】さらに、本発明に係る請求項８記載の情報認証装置によれば、データに付加された認証情報から、データを入力した装置を特定することができ、しかもその認証情報が客観性を有するので、データの証拠としての証明力をさらに向上することができるという効果も得られる。

【０２０９】さらに、本発明に係る請求項９または１０記載の情報認証装置によれば、データに付加された認証情報から、データが改ざんされているか否かが分かり、しかもその認証情報が客観性を有するので、データの証拠としての証明力をさらに向上することができるという効果も得られる。

【０２１０】さらに、本発明に係る請求項１１または１２記載の情報認証装置によれば、認証局では、受信したデータが、そのデータの送信元である情報認証装置の公開鍵でしか復号化することができないので、復号化できたときは、情報認証装置で入力したデータが確かにその

33

情報認証装置から送信されたものであるということが分かり、復号化できなかったときは、そうでないことが分かるので、データの証拠としての証明力をさらに向上することができるという効果も得られる。

【０２１１】一方、本発明に係る請求項１４ないし２３記載の認証局によれば、データに付加された認証情報が改ざんされたりデータが不正な方法で送信されたりした場合には、データにディジタル署名が付加されないので、従来に比して、データの客観性を確保することができ、データの証拠としての証明力を向上することができるという効果が得られる。

【０２１２】さらに、本発明に係る請求項１５記載の認証局によれば、データの認証情報として付加された時間情報が改ざんされた場合には、データにディジタル署名が付加されないので、データの客観性をさらに確保することができ、データの証拠としての証明力をより一層向上することができるという効果も得られる。

【０２１３】さらに、本発明に係る請求項１６記載の認証局によれば、データの認証情報として付加された位置情報が改ざんされた場合には、データにディジタル署名が付加されないので、データの客観性をさらに確保することができ、データの証拠としての証明力をより一層向上することができるという効果も得られる。

【０２１４】さらに、本発明に係る請求項１７記載の認証局によれば、データの認証情報として付加された装置情報が改ざんされた場合には、データにディジタル署名が付加されないので、データの客観性をさらに確保することができ、データの証拠としての証明力をより一層向上することができるという効果も得られる。

【０２１５】さらに、本発明に係る請求項１８または１９記載の認証局によれば、データの認証情報として付加された検査情報やデータ自体が改ざんされた場合には、データにディジタル署名が付加されないので、データの＊

34

＊客観性をさらに確保することができ、データの証拠としての証明力をより一層向上することができるという効果も得られる。

【図面の簡単な説明】

【図１】情報認証システムの構成を示すブロック図である。

【図２】情報処理装置４０の構成を示すブロック図である。

【図３】認証情報付加処理を示すフローチャートである。

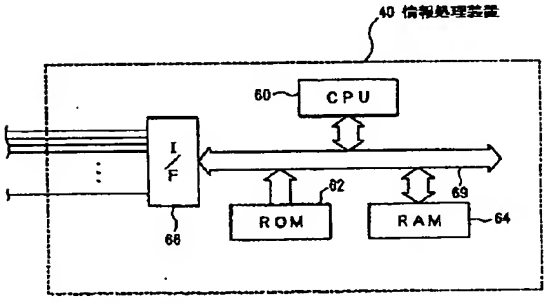
【図４】情報処理装置５０の構成を示すブロック図である。

【図５】ディジタル署名付加処理を示すフローチャートである。

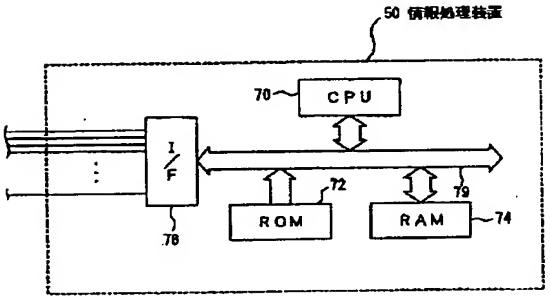
【符号の説明】

１００	情報認証装置
１２０	認証情報付加部
２００	認証局
２２０	ディジタル署名付加部
１０	ディジタルカメラ
１２，２６	個人情報入力装置
１４	個人情報記憶装置
１６，２８	装置情報記憶装置
１８，２４	通信装置
２０	データ記憶装置
４０，５０	情報処理装置
４２，５２	時間測定装置
４４，５４	位置測定装置
S_1～S_n	センサ
４６	利用者認証装置
６０，７０	ＣＰＵ
６２，７２	ＲＯＭ
６４，７４	ＲＡＭ

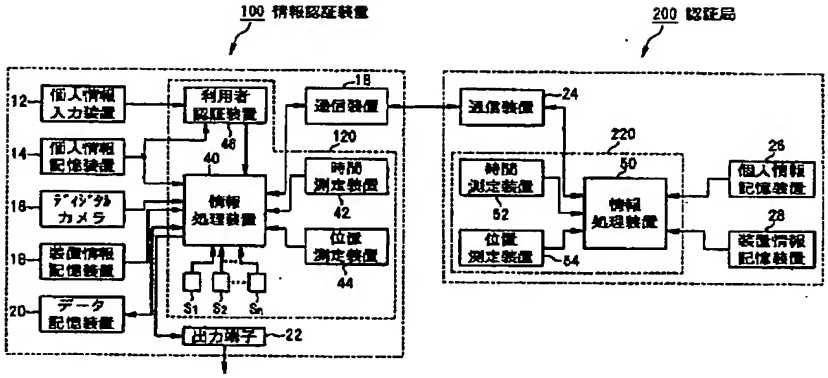
【図２】



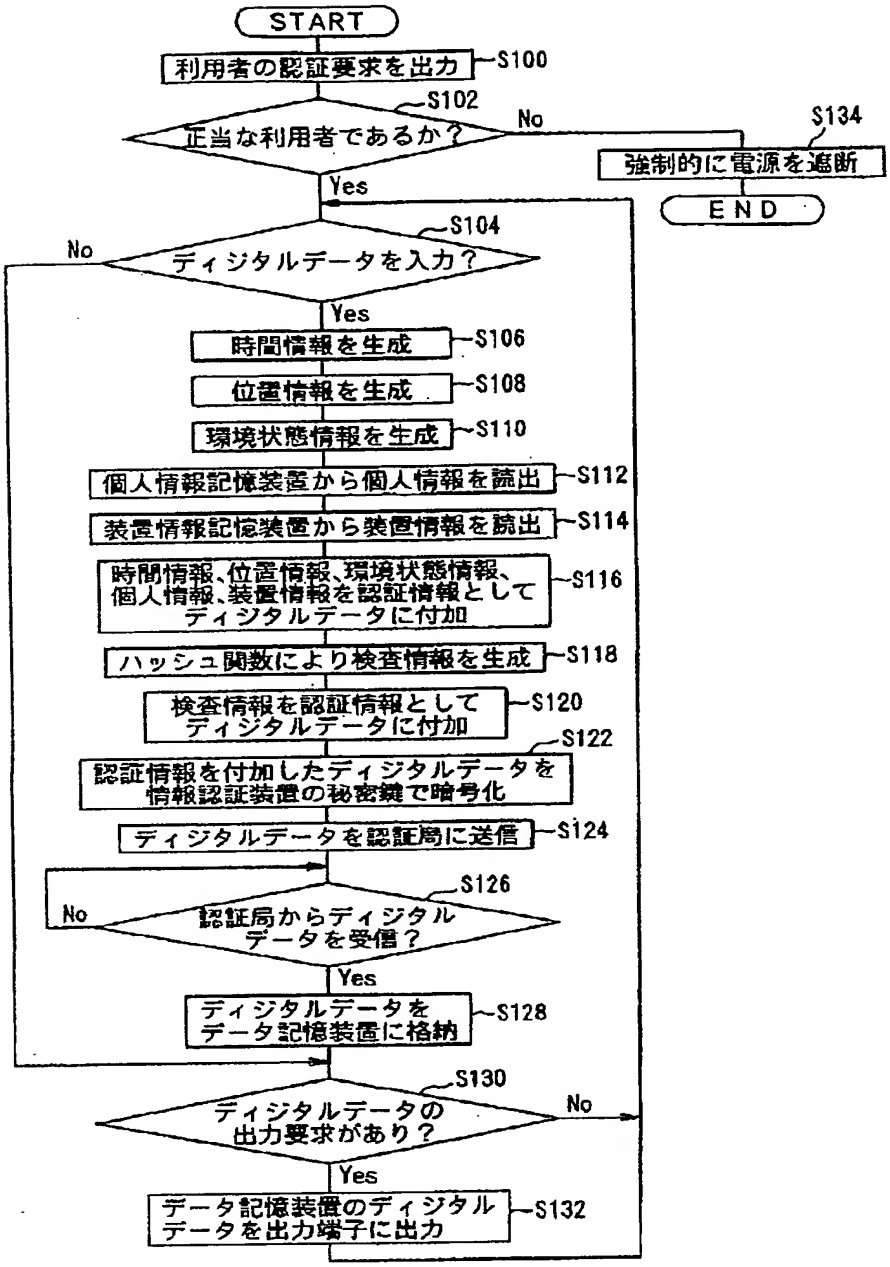
【図４】



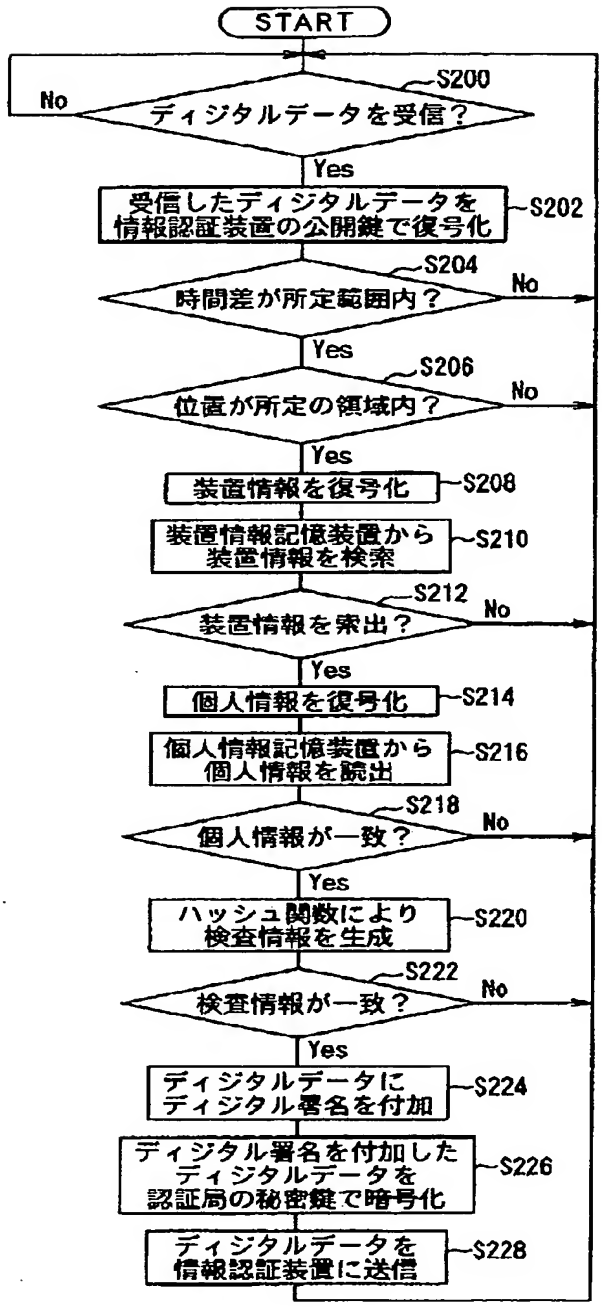
【図１】


100 情報認証装置
200 認証局
12
個人情報入力装置
14
個人情報記憶装置
16
ディジタルカメラ
18
装置情報記憶装置
20
データ記憶装置
利用者認証装置
40
48
情報処理装置
S1
S2
Sn
出力端子
22
18
通信装置
120
時間測定装置
42
位置測定装置
44
24
通信装置
220
50
時間測定装置
52
位置測定装置
54
情報処理装置
26
個人情報記憶装置
28
装置情報記憶装置

【図３】


START
利用者の認証要求を出力
S100
S102
正当な利用者であるか？
No
S134
強制的に電源を遮断
END
Yes
S104
No
ディジタルデータを入力？
Yes
時間情報を生成
S106
位置情報を生成
S108
環境状態情報を生成
S110
個人情報記憶装置から個人情報を読出
S112
装置情報記憶装置から装置情報を読出
S114
時間情報、位置情報、環境状態情報、個人情報、装置情報を認証情報としてディジタルデータに付加
S116
ハッシュ関数により検査情報を生成
S118
検査情報を認証情報としてディジタルデータに付加
S120
S122
認証情報を付加したディジタルデータを情報認証装置の秘密鍵で暗号化
ディジタルデータを認証局に送信
S124
S126
No
認証局からディジタルデータを受信？
Yes
ディジタルデータをデータ記憶装置に格納
S128
S130
ディジタルデータの出力要求があり？
No
Yes
データ記憶装置のディジタルデータを出力端子に出力
S132

【図５】


START
S200
No
ディジタルデータを受信？
Yes
受信したディジタルデータを情報認証装置の公開鍵で復号化
S202
S204
時間差が所定範囲内？
No
Yes
S206
位置が所定の領域内？
No
Yes
装置情報を復号化
S208
装置情報記憶装置から装置情報を検索
S210
S212
装置情報を索出？
No
Yes
個人情報を復号化
S214
個人情報記憶装置から個人情報を読出
S216
S218
個人情報が一致？
No
Yes
ハッシュ関数により検査情報を生成
S220
S222
検査情報が一致？
No
Yes
ディジタルデータにディジタル署名を付加
S224
ディジタル署名を付加したディジタルデータを認証局の秘密鍵で暗号化
S226
ディジタルデータを情報認証装置に送信
S228